Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions – TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Issuing Office - Bureau de distribution

Informatics Professional Services Division/Division des services professionnels en informatique
Terrasses de la Chaudière 4th Floo
10 Wellington Street
Gatineau
Quebec
K1A0S5

Title - Sujet Services d'ingénierie et d'architec	
Solicitation No. - N° de l'invitation W6369-17P5LL/B	**Date** 2019-03-19
Client Reference No. - N° de référence du client W6369-17P5LL	
GETS Reference No. - N° de référence de SEAG PW-$IPS-004-34777	
File No. - N° de dossier 004ips.W6369-17P5LL	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2019-04-09**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: Patel, Ankoor	**Buyer Id - Id de l'acheteur** 004ips
Telephone No. - N° de téléphone (613) 858-9403 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** DEPARTMENT OF NATIONAL DEFENCE 101 COLONEL BY DR. OTTAWA Ontario K1A0K2 Canada	

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Canada

DEMANDE DE SOUMISSIONS POUR LES CONTRATS CONCLUS DANS LE CADRE DE L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (AMA) POUR DES SERVICES PROFESSIONNELS EN INFORMATIQUE CENTRÉS SUR LES TÂCHES (SPICT) POUR MINISTÈRE DE LA DÉFENSE NATIONALE

Table des matières

Liste des annexes du contrat subséquent :

Annexe A Énoncé des travaux : Volet de Travail 1 – Secret
Annexe A Énoncé des travaux : Volet de Travail 2 – Très Secret

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 : Volet de Travail 1 – Secret
Appendice C de l'annexe A – Critères d'évaluation des ressources et tableau de réponses : Volet de Travail 2 – Très Secret
Appendice D de l'annexe A – Attestations à l'étape de l'autorisation de tâches

Annexe B Base de paiement
Annexe C Liste de vérification des exigences relatives à la sécurité

Appendice A de l'annexe C - Guide de sécurité complémentaire de la Liste de vérification des exigences relatives à la sécurité - Volet de Travail 1 – Secret
Appendice A de l'annexe C - Guide de sécurité complémentaire de la Liste de vérification des exigences relatives à la sécurité - Volet de Travail 2 – Très Secret

Liste des pièces jointes à la partie 3 (Instructions pour la préparation des soumissions)

- Pièce jointe 3.1 : Formulaire de présentation de la soumission

Liste des pièces jointes à la partie 4 (Procédures d'évaluation et méthode de sélection)

- Pièce jointe 4.1 : Critères d'évaluation des soumissions : Volet de Travail 1 – Secret
- Pièce jointe 4.1 : Critères d'évaluation des soumissions : Volet de Travail 2 – Très Secret
- Pièce jointe 4.2 : 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 LES CONTRATS CONCLUS DANS LE CADRE DE L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (AMA) POUR DES SERVICES PROFESSIONNELS EN INFORMATIQUE CENTRÉS SUR LES TÂCHES (SPICT) POUR MINISTÈRE DE LA DÉFENSE NATIONALE

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 et toute autre annexe.

1.2 Sommaire

(a) La présente demande de soumissions est une nouvelle demande pour le besoin décrit dans la demande nº W6369-17P5LL/A datée du 2019/02/13 et portant la date et l'heure de clôture suivantes : 2019/03/06 et 14:00 HNE*;* ce document remplace entièrement la version précédente.

(b) La présente demande de soumissions vise à répondre au besoin de Ministère de la Défense Nationale (le « **client** ») en matière de SPICT dans le cadre de l'AMA pour des SPICT.

(c) Il est prévu qu'au plus deux (2) contrats soient attribués dans chacun des deux (2) volets de travail et à ce que chaque contrat porte uniquement sur les travaux du volet qui y sont associés. Chaque contrat sera d'une durée de trois (3) ans et comprendra une (1) période irrévocable d'un (1) an qui permettra au Canada d'en prolonger la durée. Les soumissionnaires ne sont pas tenus de présenter une soumission pour chaque volet de travail. Si un soumissionnaire souhaite présenter une offre portant sur plusieurs volets de travail, une soumission technique distincte

devra être soumise pour chaque volet de travail lorsque le soumissionnaire choisit de transmettre sa soumission sur papier.

(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 nord-américain (ALENA), 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 libre-échange canadien (ALEC), et de l'Accord de partenariat transpacifique global et progressiste (PTPGP).

(f) Ce besoin est assujetti au Programme des marchandises contrôlées. La Loi sur la production de défense définit les marchandises contrôlées comme certains biens matériels figurant sur la Liste des marchandises d'exportation contrôlée, un règlement pris dans le cadre en vertu de la Loi sur les licences d'exportation et d'importation (LLEI).

(g) 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 ».

(h) 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.

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

(j) Seuls les titulaires d'AMA pour des SPICT qui détiennent actuellement un AMA pour des SPICT au palier 2, dans toutes les catégories de ressources d'un volet de travail et dans la région de la capitale nationale 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.

(k) 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 EN578-170432 au moment de la clôture des soumissions pour pouvoir présenter une soumission.

(l) 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.

VOLET DE TRAVAIL 1 – SECRET

CATÉGORIE DE RESSOURCE	TITRE PROPRE À LA TÂCHE	NIVEAU D'EXPERTISE	NOMBRE ESTIMÉ DE RESSOURCES REQUISES
Analyste des méthodes, politiques et procédures en sécurité des TI	STIG (Security Technical Implementation Guide)	NIVEAU 2	2
Spécialiste de l'ICP	ICP	NIVEAU 3	3
Ingénieur en sécurité de la TI	Sécurité réseau – Contenu	NIVEAU 3	2
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	NIVEAU 2	2
Spécialiste en conception de la sécurité de la TI	Échange d'information	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Contenu	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Sécurité de la virtualisation	NIVEAU 3	2
Spécialiste en conception de la sécurité de la TI	SES SPPEN	NIVEAU 3	1
Analyste de la sécurité des réseaux	SES SPPEN	NIVEAU 2	6
Analyste de la sécurité des réseaux	Échange d'information	NIVEAU 2	1
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	NIVEAU 3	3

VOLET DE TRAVAIL 2 – TRÈS SECRET

CATÉGORIE DE RESSOURCE	TITRE PROPRE À LA TÂCHE	NIVEAU D'EXPERTISE	NOMBRE ESTIMÉ DE RESSOURCES REQUISES
Ingénieur en sécurité de la TI	Gestion de la configuration	NIVEAU 3	1
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	NIVEAU 2	1
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	NIVEAU 3	1
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	NIVEAU 3	1
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	NIVEAU 2	2
Ingénieur en sécurité de la TI	PEI TS / Zonage TS	NIVEAU 2	1
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	NIVEAU 2	1
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	NIVEAU 2	1
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	NIVEAU 3	3
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information (PEI)	NIVEAU 3	1

Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	NIVEAU 3	1
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	NIVEAU 3	1
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	NIVEAU 3	1
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	NIVEAU 3	1
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	NIVEAU 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 (2018-05-22), 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 au Module de réception des soumissions de TPSGC au plus tard à la date, à l'heure et à l'adresse de TPSGC indiquées à la page 1 de la demande de soumissions ou par le service Connexion postel si le soumissionnaire le souhaite.

(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 5 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

(a) Tout contrat subséquent doit être interprété et régi selon les lois en vigueur Ontario, et les relations entre les parties doivent être déterminées par ces lois.

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 Données volumétriques

Les données sur le niveau estimatif d'efforts 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.

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**

(i) Si le soumissionnaire choisit d'envoyer sa soumission par voie électronique, le Canada exige de sa part qu'il respecte l'article 08 des instructions uniformisées 2003. Les soumissionnaires sont tenus de fournir leur soumission en une seule transmission. Le service Connexion postel peut recevoir plusieurs documents pouvant chacun atteindre, au maximum, 1 Go.

(ii) La soumission doit être présentée en sections distinctes, comme suit :

(A) Section I : Soumission technique

(B) Section II : Soumission financière

(C) Section III : Attestations

(iii) Pour obtenir de plus amples renseignements, veuillez consulter l'article 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-telecopieur.

(b) **Transmission d'une soumission sur support électronique (CD ou clé USB)**

(i) Si le soumissionnaire choisit de transmettre sa soumission sur support électronique par l'entremise du Module de réception des soumissions de TPSGC, le Canada demande que la soumission soit présentée en sections distinctes, comme suit :

(ii) Section I : Soumission technique – une copie électronique sur CD ou clé USB.

(iii) Section II : Soumission financière – une copie électronique DISTINCTE sur CD ou clé USB.

(iv) Section III : Attestations – une copie électronique sur CD ou clé USB.

(c) Si le soumissionnaire fournit simultanément une copie de la soumission à l'aide du service Connexion postel et une copie sur support électronique, et en cas d'incompatibilité entre le libellé de la version soumise à l'aide du service Connexion postel et celui de la version soumise sur support électronique, le libellé de la version transmise à l'aide du service Connexion postel aura préséance.

(d) Le Canada ne demande pas de copie papier de la soumission. Toutefois, si le soumissionnaire transmet une copie papier de sa soumission, et s'il y a incompatibilité entre le libellé de la copie soumise à l'aide du service Connexion postel ou sur support électronique, le libellé de la copie transmise à l'aide du service Connexion postel ou sur support électronique aura préséance sur le libellé de la copie papier.

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

(f) **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.

(g) **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 (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html). Pour aider le Canada à atteindre ses objectifs, les soumissionnaires devraient :

(i) utiliser du papier contenant des fibres certifiées provenant d'un aménagement forestier durable ou contenant au moins 30 % de matières recyclées;

(ii) utiliser un format qui respecte l'environnement : impression noir et blanc, recto verso ou à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ni reliure à anneaux.

(h) **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 une entité liée participe à plusieurs soumissions (participer signifie faire partie du soumissionnaire, et non pas être un sous-traitant), le Canada accordera deux (2) jours ouvrables à ces soumissionnaires pour indiquer la soumission unique que le Canada devra examiner. À défaut de respecter ce délai, les soumissions visées seront rejetées. Une seule soumission peut contenir des propositions visant à obtenir un contrat dans un ou plusieurs volets de travail. Cependant, une soumission ne peut pas contenir une soumission du soumissionnaire et de ses entités liées en vue d'obtenir plus d'un contrat dans l'un des volets de travail.

(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 sont pas non plus autorisés à déposer une autre soumission, que ce soit de façon autonome ou au sein d'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 3.1 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) **Exigences relatives à la sécurité** : On demande aux soumissionnaires de fournir, avec leur soumission, les renseignements de sécurité suivants pour chaque ressource proposée, avant ou à la date de clôture des soumissions.

RENSEIGNEMENTS DE SÉCURITÉ	
Nom de la personne tel qu'indiqué sur le formulaire de demande d'autorisation de sécurité	
Niveau de l'autorisation de sécurité obtenue	
Période de validité de l'attestation de sécurité obtenue	
Numéro de dossier du formulaire « Certificat d'enquête de sécurité et profil de sécurité »	

Si le soumissionnaire n'a pas inclus les renseignements de sécurité dans sa soumission, l'autorité contractante lui donnera l'occasion de fournir ces renseignements pendant la période d'évaluation. Si le soumissionnaire n'a pas fourni les renseignements de sécurité pendant la période fixée par l'autorité contractante, sa soumission sera déclarée non recevable.

(iii) **Justification de la conformité technique** : 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.

(iv) **Pour les projets antérieurs similaires** : Dans les cas où la soumission doit comprendre la description de projets antérieurs semblables : (i) le projet doit avoir été réalisé par le soumissionnaire lui-même (l'expérience acquise par un sous-traitant proposé ou une société affiliée au soumissionnaire ne compte pas); (ii) le projet doit avoir été terminé à la date de clôture des soumissions; (iii) toutes les descriptions de projet doivent comprendre, au minimum, le nom et le numéro de téléphone ou l'adresse de courriel d'un

client cité en référence; et (iv) dans l'éventualité où le soumissionnaire présente plus de projets semblables que ce qui a été demandé, le Canada aura le plein pouvoir de choisir ceux qui seront évalués. Un projet sera jugé « similaire » aux travaux à effectuer dans le cadre du contrat subséquent s'il porte sur des travaux qui correspondent étroitement aux descriptions des SPICT des catégories de ressources indiquées à l'annexe A. Les travaux seront considérés comme « correspondant étroitement » si la description du projet inclut au moins 50 % des points de responsabilité figurant dans la description de la catégorie de ressources donnée.

(v) **Pour les ressources proposées** : La soumission technique doit comprendre le nombre de curriculum vitæ, par catégorie de ressources, selon ce qui est indiqué à la pièce jointe 4.1. Une même personne ne doit pas être proposée dans plus d'une catégorie de ressources ou dans plus d'un volet de travail. La soumission technique doit démontrer que chaque personne proposée satisfait aux exigences de qualification décrites (y compris les exigences en matière d'études, d'expérience de travail, et d'accréditation professionnelle). Quant aux ressources proposées :

(A) Les ressources proposées peuvent être des employés du soumissionnaire ou d'un sous-traitant, ou il peut s'agir d'entrepreneurs indépendants auxquels le soumissionnaire attribuerait une partie du travail (voir la Partie 5, Attestations).

(B) Pour les exigences en matière d'études, de titre ou de certificat, TPSGC ne tiendra compte que des programmes ayant été réussis par la ressource à la clôture des soumissions. Si le diplôme, le titre ou le certificat a été attribué par un établissement d'enseignement à l'extérieur du Canada, on demande au soumissionnaire de fournir une copie des résultats du service d'évaluation des diplômes et de reconnaissance des compétences provenant d'une organisation ou d'un organisme reconnu par le Centre d'information canadien sur les diplômes internationaux. Si le soumissionnaire n'a pas inclus la copie des résultats dans sa soumission, l'autorité contractante lui donnera la possibilité de la fournir pendant la période d'évaluation. Si le soumissionnaire n'a pas soumis la copie des résultats dans les deux jours ouvrables suivant la demande de l'autorité contractante, sa soumission sera déclarée non recevable.

(C) En ce qui concerne les exigences relatives aux titres professionnels, la ressource doit détenir le titre exigé à la clôture des soumissions et doit demeurer, le cas échéant, un membre en règle de l'organisme professionnel ou être affiliée à l'association professionnelle 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 ou d'un diplôme, ce document doit être actuel, valide et émis par l'entité précisée dans la présente demande de soumissions. Si l'entité n'est pas précisée, l'émetteur devait être une entité, un organisme ou un établissement reconnu ou accrédité au moment où le document a été produit. Si le diplôme ou le certificat a été attribué par un établissement d'enseignement à l'extérieur du Canada, on demande au soumissionnaire de fournir une copie des résultats du service d'évaluation des diplômes et de reconnaissance des compétences provenant d'une organisation ou d'un organisme reconnu par le Centre d'information canadien sur les diplômes internationaux. Si le soumissionnaire n'a pas inclus la copie des résultats dans sa soumission, l'autorité contractante lui donnera la possibilité de la fournir pendant la période d'évaluation. Si le soumissionnaire n'a pas soumis la copie des résultats dans les deux jours ouvrables suivant la demande de l'autorité contractante, sa soumission sera déclarée non recevable.

(D) Quant à l'expérience de travail, TPSGC ne tiendra pas compte de l'expérience acquise dans le cadre d'un programme de formation, sauf s'il s'agit d'un programme Coop formel, suivi dans un établissement postsecondaire.

(E) Pour les exigences qui demandent un nombre précis d'années d'expérience (p. ex., 2 ans), TPSGC ne tiendra pas compte de cette expérience si la soumission technique 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). TPSGC n'évaluera que la période au cours de laquelle la personne a réellement travaillé au projet ou aux projets (de la date de début indiquée pour la personne 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 personne a participé.

(F) Pour que l'expérience de travail soit considérée par le Canada, la soumission technique ne doit pas seulement indiquer le titre du poste occupé par la personne, mais elle doit également démontrer que cette personne a acquis l'expérience nécessaire en expliquant les responsabilités et les tâches effectuées dans 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 les exigences de qualification, 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.

(vi) **Coordonnées des 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 (2) jours ouvrables pour fournir les renseignements requis au Canada. À défaut de respecter ce délai, la soumission sera jugée non recevable. Les clients cités en référence doivent tous confirmer, si TPSGC le demande, les renseignements requis dans les exigences obligatoires concernant l'organisation O1 pour les volets 1 et 2 de la pièce jointe 4.1.

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

Le soumissionnaire a-t-il fourni à votre organisation les services décrits ci-dessous?

Le soumissionnaire doit s'être fait octroyer au moins deux (2) contrats de service professionnel en informatique† par un client gouvernemental.*

Chacun des contrats mentionnés :

(a) *doit avoir une valeur d'au moins cinq (5) millions de dollars, taxes applicables en sus;*
(b) *doit avoir eu une durée d'au moins deux (2) ans au cours des huit (8) dernières années précédant la date de clôture de la présente demande de soumissions et ne pas comprendre les années d'option qui n'ont pas été exercées;*
(c) *doit montrer que le soumissionnaire a fourni au moins cinq (5) ressources simultanément pendant une période d'au moins douze (12) mois consécutifs.*

Chaque contrat mentionné doit également démontrer que le soumissionnaire a fourni des services à une organisation dans un milieu :

(a) doté d'au moins 100 postes de travail connectés à un réseau protégé ou secret;
(b) utilisant des systèmes d'exploitation Windows pour poste de travail (Windows XP, Windows Vista, Windows 7 ou Windows 10);
(c) faisant appel à une gestion centralisée de la distribution de logiciels et des correctifs.

**Client gouvernemental s'entend d'un ministère ou d'un organisme fédéral, provincial ou municipal ou d'une société d'État.*
†Les services professionnels en informatique sont les services professionnels fournis par le soumissionnaire pour appuyer un projet ou un marché en technologie ou en gestion de l'information.

___ *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.

Les soumissionnaires doivent 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. Les références de l'État sont acceptées.

(vii) **Profil de l'entreprise** : On demande au soumissionnaire de fournir le profil de son entreprise. Celui-ci devrait contenir un aperçu de l'entreprise, des sous-traitants ou des agents autorisés qui participeraient à l'accomplissement des tâches pour le compte du soumissionnaire. Ce dernier doit donner une brève description de l'entreprise en indiquant sa taille, sa structure organisationnelle, le nombre d'années d'activité, ses activités opérationnelles, ses principaux clients, le nombre d'employés et leur répartition géographique. Ces renseignements ne sont demandés qu'à titre informatif et ne seront pas évalués.

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 4.2. 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.

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 constituée de représentants du client et de TPSGC évaluera les soumissions au nom du Canada. Le Canada peut faire appel à des experts-conseils ou à des *personnes*-ressources du gouvernement pour évaluer les soumissions. Chaque membre de l'équipe d'évaluation ne participera pas nécessairement à tous les volets de l'évaluation.

(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 3 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.

4.2 Évaluation technique

Une évaluation technique distincte sera effectuée pour chaque volet de travail.

(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.

(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 4.1.

(c) **Nombre de ressources évaluées**

Seul un certain nombre de ressources par catégorie seront évaluées dans le cadre de la présente demande de soumissions, comme l'indique la pièce jointe 4.1. Les autres 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 n'est pas obligatoire. Toutefois, si TPSGC choisit de le faire pour quelque exigence cotée ou obligatoire que ce soit, il vérifiera les références des 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 à toutes les personnes dont les coordonnées ont été fournies par les soumissionnaires, dans une période de 48 heures, à l'aide des adresses électroniques indiquées dans la soumission. La réponse doit être envoyée dans les cinq (5) 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) Si le client cité en référence ne répond pas dans les cinq (5) jours ouvrables, le Canada ne communiquera pas avec le soumissionnaire; 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, l'information donnée par la personne citée en référence sera vérifiée.

(v) On n'accordera aucun point ou on ne considérera pas qu'un critère d'expérience obligatoire a été respecté (le cas échéant) 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 que 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 on considérera qu'un critère obligatoire n'est pas respecté si le client est lui-même une filiale ou autre entité qui a des liens de dépendance avec le soumissionnaire.

4.3 Évaluation financière

a) Deux méthodes d'évaluation financière sont possibles pour ce besoin. La première méthode sera utilisée lorsque trois soumissions ou plus sont jugées recevables (voir le point b) – Évaluation financière – Méthode A, ci-dessous). La seconde méthode sera utilisée s'il y a moins de

trois soumissions recevables (voir le point d) – Évaluation financière – Méthode B, ci-dessous). Un prix de l'évaluation financière distinct sera calculé pour chaque volet de travail.

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

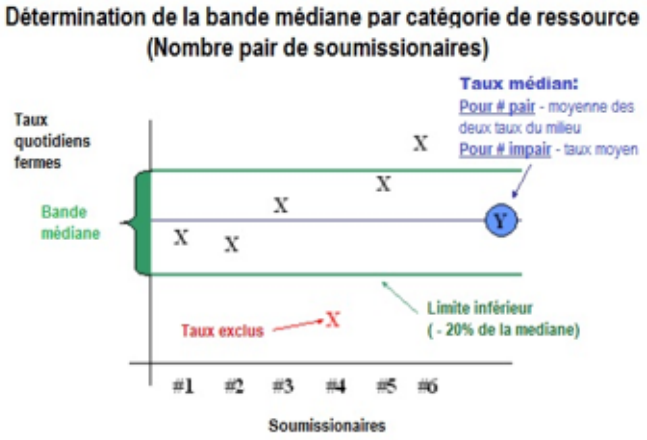
(i) Calcul du prix total de la soumission : L'évaluation financière sera effectuée à partir des tableaux d'établissement des prix fournis par les soumissionnaires et de la méthode d'évaluation de la médiane des taux quotidiens fermes expliquée ci-dessous. On effectuera des calculs financiers pour chaque soumissionnaire en multipliant les taux fermes quotidiens, ou les taux médians s'il y a lieu, pour la période initiale du contrat et les périodes d'option par le nombre prévu de jours de travail pour chaque période, dans toutes les catégories de ressource énoncées dans la pièce jointe 4.2 – Barème de prix. La somme de ces taux représente le prix total de la soumission pour ce soumissionnaire.

(ii) Évaluation de la médiane des taux quotidiens fermes

(A) Méthode utilisée : La médiane des taux quotidiens fermes servira à modifier le taux à évaluer lors de l'évaluation financière d'un soumissionnaire, lorsqu'un soumissionnaire propose un taux quotidien ferme pour une catégorie de ressource qui est inférieur à la limite inférieure de la bande établie selon le calcul ci-après. Le calcul de la médiane du taux quotidien ferme servira aux fins d'évaluation seulement, et le taux quotidien réel soumis sera utilisé dans le cadre du contrat subséquent, dans tous les cas.

(B) Calcul des médianes pour la période initiale du contrat et les périodes d'option : Une bande médiane sera calculée pour chaque catégorie de ressources à l'aide du taux quotidien proposé pour chaque ressource individuelle, et pour chacune des périodes d'option. Le taux médian pour chaque catégorie de ressources sera calculé au moyen de la fonction « médiane » de Microsoft Excel. Une limite inférieure de la bande médiane sera calculée pour chaque catégorie de ressource et permettra d'établir une fourchette qui prendra en compte un taux médian correspondant à une valeur de moins (-) 20 % du taux médian. Si un soumissionnaire propose un taux quotidien ferme pour une catégorie de personnel, qui est inférieur à la limite inférieure de la bande, sa proposition financière sera évaluée à l'aide du taux quotidien de la limite inférieure de la bande médiane pour cette catégorie de personnel.

Par exemple, s'il est déterminé que le taux médian (Y) pour une catégorie de ressources est de 500 $, la limite inférieure de la bande médiane serait de moins (-) 20 % de 500 $, ou 400 $. Si un soumissionnaire propose un taux quotidien ferme inférieur à 400 $, le taux médian de 500 $ sera utilisé dans son évaluation financière pour cette catégorie de ressources.



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

(i) **Calcul du prix total de la soumission :** L'évaluation financière sera effectuée à partir des tableaux d'établissement des prix fournis par les soumissionnaires. On effectuera des calculs financiers pour chaque soumissionnaire en multipliant les taux fermes quotidiens pour la période initiale du contrat et les périodes d'option par le nombre prévu de jours de travail pour chaque période, dans toutes les catégories de personnel énoncées dans la pièce jointe 4.2 – Barème de prix. La somme de ces taux représente le prix total de la soumission pour ce soumissionnaire.

d) 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 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) pour chacun des contrats pour lesquels une facture est présentée à titre de justification, le curriculum vitæ de la ressource qui a offert les services dans le cadre de ce contrat afin de démontrer que la ressource répondrait aux exigences obligatoires et obtiendrait la note de passage pour tous les critères cotés de la catégorie de ressource faisant l'objet d'une justification des taux;

(iv) 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.

e) 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

Processus de sélection : le processus de sélection suivant sera suivi pour chaque volet de travail.

(a) 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.

(b) 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.

(i) Calcul de la note technique totale : pour chaque volet, 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).

$$\frac{\text{Note technique}}{\text{Note technique maximale (soumissionnaires, veuillez consulter la note technique maximale à la pièce jointe 4.1.)}} \times 70 = \text{note technique totale}$$

(ii) Calcul de la note financière totale : pour chaque volet, 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).

$$\frac{\text{Prix évalué le plus bas}}{\text{Prix évalué du soumissionnaire}} \times 30 = \text{note financière finale}$$

(iii) Calcul de la note totale du soumissionnaire : la note totale du soumissionnaire sera calculée pour chaque soumission recevable selon la formule suivante.

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

(c) Dans l'éventualité où des soumissionnaires obtiennent la même note totale, le soumissionnaire ayant obtenu la note financière finale la plus élevée sera classé au premier rang.

(d) Deux (2) contrats au plus peuvent être attribués à la suite de la présente demande de soumissions.

(e) 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 le soumissionnaire peut avoir été recommandé pour l'attribution d'un contrat, un contrat sera émis 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.

(f) **Attribution de financement pour le contrat :** lorsque plus d'un contrat est attribué pour un volet de travail, chaque contrat pour ce volet de travail particulier sera attribué selon un montant de financement précisé à l'article intitulé « Limitation des dépenses » et calculé en fonction de ce qui suit :

(i) Lorsqu'un contrat est attribué, le montant de la limitation des dépenses sera déterminé à la discrétion du Canada.

(ii) Lorsque deux contrats sont attribués, le montant de la limitation des dépenses de chaque contrat sera déterminé conformément à ce qui suit :

(A) le soumissionnaire ayant obtenu la note totale la plus élevée recevra 55 % du financement affecté initialement à ce volet de travail;

(B) le soumissionnaire ayant obtenu la deuxième note totale la plus élevée recevra 45 % du financement affecté initialement à ce volet de travail.

(g) 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 le soumissionnaire peut avoir été recommandé pour l'attribution d'un contrat, un contrat sera émis 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 Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, remplie pour chaque membre de la coentreprise.

5.2 Attestations supplémentaires préalables à l'attribution du contrat

(a) Services professionnels – Ressources

(i) En présentant une soumission, le soumissionnaire atteste que, s'il obtient le contrat, chaque individu proposé dans sa soumission sera disponible pour exécuter les travaux, tel qu'il est exigé par les représentants du Canada, au moment indiqué dans la demande de soumissions ou convenu avec ces derniers.

(ii) En déposant une soumission, le soumissionnaire atteste qu'il a vérifié tous les renseignements fournis dans les curriculum vitæ et les documents à l'appui présentés avec sa soumission, plus particulièrement les renseignements relatifs aux études, aux réalisations, à l'expérience et aux antécédents professionnels, et que ceux-ci sont exacts. En outre, il garantit que chaque personne proposée est en mesure d'exécuter les travaux prévus dans le contrat subséquent.

(iii) Si le soumissionnaire a proposé une personne qui n'est pas un de ses employés, en déposant une soumission, il atteste qu'il a la permission de la personne d'offrir ses services pour l'exécution des travaux et de soumettre son curriculum vitæ au Canada. Le soumissionnaire doit, à la demande de l'autorité contractante, fournir une confirmation écrite, signée par la personne, de la permission donnée au soumissionnaire ainsi que de sa disponibilité. Le défaut de répondre à la demande peut avoir pour conséquence de rendre la soumission non recevable.

(b) Attestation linguistique – anglais essentiel

En déposant une soumission, le soumissionnaire atteste que, s'il obtient le contrat découlant de la demande de soumissions, chaque personne proposée dans sa soumission :

maîtrise l'anglais. Les personnes proposées doivent être en mesure de communiquer en anglais tant à l'oral qu'à l'écrit, sans aide, et en faisant peu d'erreurs.

(c) 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;

(iii) 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;

(b) 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.

(c) 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).

(d) 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.

6.3 Exigences relatives aux marchandises contrôlées

(a) Clause du Guide des CCUA A9130T (2014-11-27) Programme des marchandises Contrôlées

(b) Dans le cas des coentreprises, chaque membre de la coentreprise doit respecter les exigences du Programme des marchandises contrôlées.

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.*

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 Ministère de la Défense Nationale.

(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) **Attribution des autorisations de tâches :**

(i) Plus d'un contrat a été attribué pour ce besoin. Par conséquent, l'attribution des autorisations de tâches dans le cadre de la série de contrats sera conforme à ce qui suit :

(ii) Au moment où la série de contrats a été attribuée, chaque entrepreneur a reçu un montant de financement précisé dans l'article intitulé « Limitation des dépenses » en ce

qui concerne les autorisations de tâches, selon le processus d'évaluation décrit dans la demande de soumissions qui a mené à l'attribution de la série de contrats.

(iii) Le Canada fera un effort raisonnable pour veiller à ce que la valeur des autorisations de tâches émises aux entrepreneurs soit équilibrée pendant la période du contrat en fonction du financement attribué. Un examen des autorisations de tâches attribuées aux entrepreneurs sera réalisé à des intervalles de six mois et au début de chaque exercice financier, afin de confirmer que les autorisations de tâches sont utilisées et distribuées de façon proportionnelle. Si un entrepreneur refuse une autorisation de tâches dans le cadre du contrat ou que le Canada détermine que les ressources proposées ne satisfont pas aux exigences minimales en matière d'expérience ou à d'autres exigences des catégories précisées dans le projet d'autorisation de tâches, cette autorisation de tâches sera offerte à l'entrepreneur suivant, selon le même processus d'affectation. La valeur de l'autorisation de tâches refusée sera soustraite de la valeur du contrat de l'entrepreneur, et pourra être réaffectée en tout ou en partie, à la discrétion de l'autorité contractante, à un ou à plusieurs entrepreneurs du même volet. Si tous les entrepreneurs refusent une autorisation de tâches en vertu du contrat, le Canada se réserve le droit de recourir à d'autres méthodes d'approvisionnement.

c) **Évaluation 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.

d) **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 A.

(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 tâche;

(B) 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);

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

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

(E) les dates de début et de fin;

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

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

(H) le nombre de jours-personnes requis;

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

(J) le profil linguistique des ressources requises;

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

(L) 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);

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

e) **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.

f) **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 dont la valeur est inférieure ou égale à _____ $ (excluant les taxes applicables) doit être signée par le responsable technique;

(ii) toute autorisation de tâches dont la valeur est supérieure à ce montant doit être signée par le responsable technique et l'autorité contractante.

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.

g) **Administration du processus d'autorisation de tâches pour le MDN** : L'administration du processus d'autorisation de tâches sera effectuée par _____. Ce processus comprend la surveillance, le contrôle et le rapport des dépenses dans le cadre du contrat comportant des autorisations de tâches à l'intention de l'autorité contractante.

h) **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 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 10 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.

i) **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

(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 (2018-06-21), 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) 4006 (2010-08-16), Conditions générales supplémentaires – L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux;

(iii) 4008 (2008-12-12), Conditions générales supplémentaires – Renseignements personnels;

s'appliquent au contrat et en font partie intégrante.

7.5 Exigences relatives à la sécurité

VOLET DE TRAVAIL 1 – SECRET

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN: DOSSIER TPSGC Nº W6369-17-P5LL-S1 Révisé #2 Correction

(a) 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 **OTAN SECRET**, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de **Travaux publics et Services gouvernementaux Canada (TPSGC).**

(b) Ce contrat comprend un accès à des **marchandises contrôlées.** Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de **Travaux publics et Services gouvernementaux Canada (TPSGC).**

(c) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens **PROTÉGÉ/CLASSIFIÉS** ou à des établissements de travail dont l'accès est réglementé **doivent être citoyens du Canada ou des États-Unis d'Amérique** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **OTAN SECRET**, délivrée ou approuvée par la DSIC de TPSGC.

(d) L'entrepreneur ou l'offrant NE DOIT PAS emporter de renseignements ou de biens PROTÉGÉ/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.

(e) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS OTAN, ou à des établissements de travail dont l'accès est réglementé, doivent être citoyens du **Canada ou États-Unis d'Amérique** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **OTAN SECRET**, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

(f) Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la Participation, le contrôle et l'influence étrangers (PCIE) ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements

CLASSIFÉS DE L'OTAN. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

(g) En permanence pendant l'exécution du contrat, l'entrepreneur doit détenir une lettre de TPSGC indiquant les résultats de l'évaluation de la PCIE ainsi que le statut attribué à son entreprise, c'est-à-dire « Sans PCIE » ou « Sans PCIE par atténuation ».

(h) Tout changement au questionnaire et aux facteurs connexes d'évaluation de la PCIE doit être immédiatement signalé au Secteur de la sécurité industrielle (SSI) aux fins de détermination de l'incidence du changement sur le statut lié à la PCIE.

(i) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent pas être attribués sans l'autorisation écrite préalable de la DSIC de TPSGC.

(j) L'entrepreneur ou l'offrant doit respecter les dispositions:

i. 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 C;
ii. du *Manuel de la sécurité industrielle* (dernière édition).

VOLET DE TRAVAIL 2 – TRÈS SECRET

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN : DOSSIER TPSGC Nº W6369-17-P5LL-S2 Révisé #2

(k) 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 **TRES SECRET et OTAN SECRET**, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

(l) Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

(m) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉ/CLASSIFIÉS ou à des établissements de travail dont l'accès est réglementé doivent être **citoyens du Canada** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **TRES SECRET et OTAN SECRET**, délivrée ou approuvée par la DSIC de TPSGC.

(n) L'entrepreneur ou l'offrant NE DOIT PAS emporter de renseignements ou de biens CLASSIFIÉS/PROTÉGÉS 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.

(o) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS OTAN, ou à des établissements de travail dont l'accès est réglementé, **doivent être citoyens du Canada** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **OTAN SECRET**, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

(p) Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la Participation, le contrôle et l'influence étrangers (PCIE) ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements **CLASSIFÉS DE L'OTAN**. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

(q) En permanence pendant l'exécution du contrat, l'entrepreneur doit détenir une lettre de TPSGC indiquant les résultats de l'évaluation de la PCIE ainsi que le statut attribué à son entreprise, c'est-à-dire « Sans PCIE » ou « Sans PCIE par atténuation ».

(r) Tout changement au questionnaire et aux facteurs connexes d'évaluation de la PCIE doit être immédiatement signalé au Secteur de la sécurité industrielle (SSI) aux fins de détermination de l'incidence du changement sur le statut lié à la PCIE.

(s) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent pas être attribués sans l'autorisation écrite préalable de la DSIC de TPSGC.

(t) L'entrepreneur ou l'offrant doit respecter les dispositions :

i. 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 C;
ii. du *Manuel de la sécurité industrielle* (dernière édition).

7.6 Durée du contrat

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

(i) la « **durée initiale du contrat** », qui commence à la date d'attribution du contrat et qui prend fin trois (3) ans 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 une (1) période supplémentaire d'une (1) année, selon les mêmes conditions. L'entrepreneur accepte que pendant la durée prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la base de paiement.

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

7.7 Responsables

(a) Autorité contractante

L'autorité contractante dans le cadre du contrat est :

Nom : Ankoor Patel
Titre : Spécialiste en approvisionnement
Travaux publics et Services gouvernementaux Canada
Direction générale des approvisionnements
Direction : Direction de l'acquisition de systèmes informatiques et de télécommunications
Adresse : 11, rue Laurier, Gatineau (Québec)
Téléphone : 613-858-9403
Courriel : Ankoor.patel@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

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.

(c) **Représentant de l'entrepreneur**

[Remplir ou supprimer, selon le cas.]

7.8 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.

7.9 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) **Frais de déplacement et de subsistance – Directive sur les voyages du Conseil national mixte :** L'entrepreneur sera remboursé pour ses 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 le profit ou les frais administratifs généraux, conformément aux indemnités relatives aux repas et à l'utilisation d'un véhicule qui sont précisés 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 se rapportent aux « voyageurs » plutôt que celles qui se rapportent aux « employés ». Tout déplacement doit être approuvé au préalable par le responsable technique. Les demandes de voyage seront prises en compte uniquement pour un lieu de travail situé à plus de 100 kilomètres de l'installation du MDN dans la RCN. L'entrepreneur sera payé pour les heures consacrées au déplacement en fonction de la moitié du taux horaire. Le taux horaire sera déterminé en divisant le taux quotidien ferme établi à l'annexe B par 7,5 heures. Tous les paiements peuvent faire l'objet d'une vérification par le gouvernement.

(iii) **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.

(iv) **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.

(v) **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**

(i) Dans le cadre du contrat, la responsabilité totale du Canada envers l'entrepreneur ne doit pas dépasser la somme indiquée à la première page du contrat, taxes applicables en sus, selon le cas. En ce qui concerne le montant inscrit à la première page du contrat, les droits de douane sont exclus, et les taxes applicables sont incluses. Les engagements d'acquisition de biens ou de services aux montants indiqués sont décrits ailleurs dans le contrat.

(ii) Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux découlant de tout changement de conception, de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements de conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrées aux travaux. L'entrepreneur ne doit pas exécuter des travaux ou fournir des services qui entraîneraient une augmentation de la responsabilité totale du Canada à moins d'obtenir par écrit l'approbation de l'autorité contractante. L'entrepreneur doit informer, par écrit, l'autorité contractante concernant la suffisance de cette somme :

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

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

(C) dès que l'entrepreneur juge que les fonds du contrat sont insuffisants pour l'achèvement des travaux,

selon la première éventualité.

(iii) 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) **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.

(e) **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.

(f) **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 ou de la fermeture des 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 des 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.

7.10 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 ainsi que deux copies de chaque facture, et une copie à l'autorité contractante.

7.11 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.

7.12 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.

7.13 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur Ontario, et les relations entre les parties doivent être déterminées par ces lois.

7.14 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) 4006 (2010-08-16), Conditions générales supplémentaires – L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux,

(iii) 4008 (2008-12-12), Conditions générales supplémentaires – Renseignements personnels;

(c) les conditions générales 2035 *(*2018-06-21*)* – 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).*

7.15 Contrat de défense

(a) Clause du guide des CCUA A9006C (2017-07-16) Contrat de défense

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 Programme de marchandises contrôlées

(a) Clause du guide des CCUA A9131C (2014-11-27) Programme des marchandises contrôlées

(b) Clause du guide des CCUA B4060C (2011-05-16) Marchandises contrôlées

7.20 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).

7.21 Entrepreneur en coentreprise

(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.*

7.22 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.

7.23 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 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.

7.25 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.

7.26 Services de transition à la fin du contrat

(a) L'entrepreneur convient que, durant la période menant à la fin du contrat, il réalisera la totalité des tâches de transition qui sont énoncées à l'annexe A de l'Énoncé des travaux et assurera la transition entre ce contrat et le nouveau contrat conclu avec un autre fournisseur. Au moyen d'une autorisation de tâches valide, les services de transition exécutés en vertu du contrat seront fournis « sur demande » et les ressources seront utilisées aux taux journaliers fermes, tout compris, énoncés à l'annexe B – Base de paiement.

(b) Les services de transition à la fin du contrat sont fournis au cours de la période commençant lorsque le MDN conclut une nouvelle entente contractuelle ou autre pour la prestation de services de génie et d'architecture en GI-TI au MDN avant la fin de la période contractuelle. Cela comprend les activités que l'entrepreneur devra entreprendre pour assurer la transition harmonieuse, efficace et complète sans interrompre le soutien au MDN.

(c) À la demande du responsable technique, l'entrepreneur devra soumettre un plan de transition de sortie exhaustif afin d'assurer de façon efficace, complète et sécurisée :

(i) la transition des services au MDN ou à un tiers choisi par le MDN;
(ii) la transition de tous les biens appartenant au Canada (y compris le code source de l'application, la base de données et les données complètes, dont les rapports stockés) au MDN ou à un tiers choisi par le MDN ;
(iii) L'entrepreneur doit transmettre le plan de transition de sortie au plus tard dix (10) jours ouvrables suivant le début des services de transition à la fin de la durée du contrat.

(d) Après l'approbation du plan de transition de sortie par le responsable technique, l'entrepreneur doit s'acquitter de toutes les obligations du plan selon le calendrier faisant partie du plan accepté par le MDN. De plus :

(i) l'entrepreneur doit assurer le transfert des connaissances au MDN ou au tiers mandaté par le MDN, selon le calendrier et selon la méthode prévue dans le plan de transition de sortie et acceptée par le MDN;
(ii) l'entrepreneur doit répondre aux questions concernant les activités de transition de sortie et tous les travaux en cours afin d'assurer une transition harmonieuse pour le MDN ou le tiers qu'il a mandaté, ainsi que d'assurer la prestation ininterrompue des services;
(iii) au cours de la période de transition de sorite, l'entrepreneur doit offrir un soutien complet et continu en matière de services de génie et d'architecture en GI-TI au MDN, en plus d'achever tous les travaux en cours, conformément au plan de transition de sortie.

7.27 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

VOLET DE TRAVAIL 1 – SECRET

Le document suit au format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à ankoor.patel@tpsgc-pwgsc.gc.ca

ANNEXE A

ÉNONCÉ DES TRAVAUX

VOLET DE TRAVAIL 2 – TRÈS SECRET

Le document suit au format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à ankoor.patel@tpsgc-pwgsc.gc.ca

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 conformément à la méthode d'attribution indiquée dans l'article du contrat intitulé « Attribution des autorisations de tâches ». 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. Pour chaque proposition de prix, l'entrepreneur doit proposer le nombre de ressources nécessaires, et pour chaque ressource proposée, l'entrepreneur doit fournir un curriculum vitæ ainsi que les renseignements sur l'attestation de sécurité exigée et remplir les tableaux de réponse joints à l'appendice C de l'annexe A, qui portent sur les catégories de ressources indiquées dans la version préliminaire de l'autorisation de tâches. La même personne ne peut être proposée pour plus d'une catégorie de ressources. Les curriculum vitæ doivent montrer que chaque personne proposée répond aux exigences décrites concernant les qualifications (y compris les exigences en matière d'études, d'expérience de travail et d'accréditation ou d'affiliation professionnelle). Les curriculum vitae doivent également montrer que la ressource proposée satisfait aux autres exigences indiquées dans l'autorisation de tâches. 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 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 (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

All invoices/progress claims must show the referenced Contract and Task numbers. Toutes les factures doivent indiquer les numéros du contrat et de la tâche.		Contract no. - No du contrat
		Task no. - No de la tâche
Amendment no. - No de la modification	Increase/Decrease - Augmentation/Réduction	Previous value - Valeur précédente
To - À	**TO THE CONTRACTOR** You are requested to supply the following services in accordance with the terms of the above referenced Contract. Only services included in the Contract can be supplied against this task. Please advise the undersigned if the completion date cannot be met. Invoices/progress claims shall be prepared in accordance with the instructions set out in the contract. À L'ENTREPRENEUR Vous êtes prié de fournir les services suivants en conformité des termes du contrat mentionné ci-dessus. Seules les services mentionnés dans le contrat doivent être fournis à l'appui de cette demande. Prière d'aviser le signataire si la livraison ne peut se faire dans les délais prescrits. Les factures doivent être établies selon les instructions énoncées dans le contrat. _____ _____ Date for the Department of National Defence pour le ministère de la Défence nationale	
Delivery location - Expédiez à		
Delivery/Completion date - Date de livraison/d'achèvement From - De : To - À :		

Contract item no. No d'article du contrat	Services	Cost Prix
	Applicable Taxes **Taxes applicables**	
	Total	
	THE CONTRACTOR HEREBY ACCEPTS THE TASK AUTHORIZATION IDENTIFIED ABOVE : _____ _____ Name (type or print) Title (type or print) _____ _____ Signature Date	

APPLICABLE ONLY TO PWGSC CONTRACTS: The Contracting Authority signature is required when the total value of the DND 626 exceeds the threshold specified in the Contract.

NE S'APPLIQUE QU'AUX CONTRATS DE TPSGC : La signature de l'autorité contractante est requise lorsque la valeur totale du formulaire DND 626 est supérieure au seuil précisé dans le contrat.

_____
for the Department of Public Works and Government Services
pour le ministère des Travaux publics et services gouvernementaux

DND 626 (01-05)

APPENDICE C DE L'ANNEXE A
CRITÈRES D'ÉVALUATION DES RESSOURCES ET TABLEAU DE RÉPONSE
VOLET DE TRAVAIL 1 – SECRET

Le document suit au format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à ankoor.patel@tpsgc-pwgsc.gc.ca

APPENDICE C DE L'ANNEXE A
CRITÈRES D'ÉVALUATION DES RESSOURCES ET TABLEAU DE RÉPONSE
VOLET DE TRAVAIL 2 – TRÈS SECRET

Le document suit au format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à ankoor.patel@tpsgc-pwgsc.gc.ca

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

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

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.

_____ _____

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

ANNEXE B

BASE DE PAIEMENT

VOLET DE TRAVAIL 1 :

Catégorie de ressources	Titre propre à la tâche	Niveau	Période du contrat 1 (AN. 1)	Période du contrat 2 (AN. 2)	Période du contrat 3 (AN. 3)	Période d'option 1 (AN. 4)
Analyste des méthodes, politiques et procédures en sécurité des TI	STIG (Security Technical Implementation Guide)	2				
Spécialiste de l'ICP	ICP	3				
Ingénieur en sécurité de la TI	Sécurité réseau – Inspection du contenu	3				
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2				
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information	3				
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3				
Spécialiste en conception de la sécurité de la TI	Sécurité de la virtualisation	3				
Spécialiste en conception de la sécurité de la TI	SES SPPEN	3				
Analyste de la sécurité des réseaux	SES SPPEN	2				
Analyste de la sécurité des réseaux	Passerelle d'échange d'information	2				
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3				

VOLET DE TRAVAIL 2 :

Catégorie de ressources	Titre propre à la tâche	Niveau	Période du contrat 1 (AN. 1)	Période du contrat 2 (AN. 2)	Période du contrat 3 (AN. 3)	Période d'option 1 (AN. 4)
Ingénieur en sécurité de la TI	Gestion de la configuration	3				
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	2				
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	3				
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	3				
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	2				
Ingénieur en sécurité de la TI	PEI TS/Zonage TS	2				
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	3				
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	2				
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2				
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	3				
Spécialiste en conception	Passerelle d'échange	3				

de la sécurité de la TI	d'information (PEI)					
Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	3				
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	3				
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3				
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	3				
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3				
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	3				
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	3				

ANNEXE C

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

VOLET DE TRAVAIL 1 ET VOLET DE TRAVAIL 2

Vous trouverez les documents ci-après en format PDF.

APPENDICE A DE L'ANNEXE C

Guide de sécurité complémentaire de la Liste de vérification des exigences relatives à la sécurité - Volet de Travail 1 – Secret

Vous trouverez les documents ci-après en format PDF.

APPENDICE A DE L'ANNEXE C

Guide de sécurité complémentaire de la Liste de vérification des exigences relatives à la sécurité - Volet de Travail 2 – Très Secret

Vous trouverez les documents ci-après en format PDF.

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	
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. **(Remarque : Les agents d'approvisionnement devraient supprimer cette exigence si elle n'est pas incluse dans la Partie 6.)**	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	Le soumissionnaire est-il un ancien fonctionnaire touchant une pension tel qu'il est défini dans la demande de soumissions?	

<table>
<tr><td rowspan="2">fonctionnaire », dans la Partie 2 de la demande de soumissions.</td><td colspan="2">Oui ____ Non ____
Si oui, fournir les renseignements demandés à l'article intitulé « Ancien fonctionnaire » dans la Partie 2.</td></tr>
<tr><td colspan="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.</td></tr>
<tr><td rowspan="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.]</td><td colspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">Volet de travail couvert par la présente soumission : Les soumissionnaires doivent indiquer quel volet de travail ils proposent d'approvisionner dans cette soumission (si le soumissionnaire a présenté une offre pour un ou plusieurs volets de travail, indiquez uniquement le volet de travail couvert par la présente soumission).</td><td>Volet de travail</td><td>Oui/Non</td></tr>
<tr><td>Volet de travail 1</td><td></td></tr>
<tr><td>Volet de travail 2</td><td></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td>Signature du représentant autorisé du soumissionnaire</td><td colspan="2"></td></tr>
</table>

PIÈCE JOINTE 4.1
CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 1 – SECRET

Vous trouverez ci-joint les critères d'évaluation des soumissions en format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à Ankoor.patel@tpsgc-pwgsc.gc.ca.

PIÈCE JOINTE 4.1
CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 2 – TRÈS SECRET

Vous trouverez ci-joint les critères d'évaluation des soumissions en format PDF.

Une version en format Word est disponible sur demande en envoyant un courriel directement à Ankoor.patel@tpsgc-pwgsc.gc.ca.

PIÈCE JOINTE 4.2
BARÈME DE PRIX

En ce qui concerne le « nombre estimatif de jours » indiqué ci-dessous dans la colonne (C*), ce nombre sert uniquement aux fins d'évaluation pendant le processus de demande de soumissions et ne représente pas un engagement relatif à une utilisation future.

VOLET DE TRAVAIL 1 :

Période initiale du contrat :

Période du contrat un (AN. 1)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Analyste des méthodes, politiques et procédures en sécurité des TI	STIG (Security Technical Implementation Guide)	2	300	$	$
Spécialiste de l'ICP	ICP	3	720	$	$
Ingénieur en sécurité de la TI	Sécurité réseau – Inspection du contenu	3	480		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	300		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de	Sécurité de la virtualisation	3	300		

la sécurité de la TI					
Spécialiste en conception de la sécurité de la TI	SES SPPEN	3	240		
Analyste de la sécurité des réseaux	SES SPPEN	2	720		
Analyste de la sécurité des réseaux	Passerelle d'échange d'information	2	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	720		
	Prix total pour la période contractuelle un				**<À déterminer> $**

Période du contrat deux (AN. 2)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Analyste des méthodes, politiques et procédures en sécurité des TI	STIG (Security Technical Implementation Guide)	2	420	$	$
Spécialiste de l'ICP	ICP	3	720	$	$
Ingénieur en sécurité de la TI	Sécurité réseau – Inspection du contenu	3	480		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	420		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information	3	240		

Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité de la virtualisation	3	420		
Spécialiste en conception de la sécurité de la TI	SES SPPEN	3	240		
Analyste de la sécurité des réseaux	SES SPPEN	2	1200		
Analyste de la sécurité des réseaux	Passerelle d'échange d'information	2	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	720		
	Prix total pour la période contractuelle deux				**<À déterminer> $**

Période du contrat trois (AN. 3)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Analyste des méthodes, politiques et procédures en sécurité des TI	STIG (Security Technical Implementation Guide)	2	480	$	$
Spécialiste de l'ICP	ICP	3	720	$	$
Ingénieur en sécurité de la TI	Sécurité réseau – Inspection du contenu	3	480		

Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	480		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité de la virtualisation	3	480		
Spécialiste en conception de la sécurité de la TI	SES SPPEN	3	240		
Analyste de la sécurité des réseaux	SES SPPEN	2	1440		
Analyste de la sécurité des réseaux	Passerelle d'échange d'information	2	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	720		
	Prix total pour la période contractuelle trois				**<À déterminer> $**

Périodes d'option :

Période d'option un (AN. 4)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Analyste des méthodes, politiques et	STIG (Security Technical	2	480	$	$

procédures en sécurité des TI	Implementation Guide)				
Spécialiste de l'ICP	ICP	3	720	$	$
Ingénieur en sécurité de la TI	Sécurité réseau – Inspection du contenu	3	480		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	480		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité de la virtualisation	3	480		
Spécialiste en conception de la sécurité de la TI	SES SPPEN	3	240		
Analyste de la sécurité des réseaux	SES SPPEN	2	1440		
Analyste de la sécurité des réseaux	Passerelle d'échange d'information	2	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	720		
	Prix total pour la période contractuelle quatre				**<À déterminer> $**

Prix total de la soumission :	
(Prix total de la période du contrat un + Prix total de la période du contrat deux + Prix total de la période du contrat trois + Prix total de la période d'option un)	**<À déterminer> $**

VOLET DE TRAVAIL 2 :

Période initiale du contrat :

Période du contrat un (AN. 1)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Ingénieur en sécurité de la TI	Gestion de la configuration	3	240	$	$
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	2	240	$	$
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	2	480		
Ingénieur en sécurité de la TI	PEI TS / Zonage TS	2	240		
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	3	240		
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	2	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	240		
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	3	720		

Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information (PEI)	3	240		
Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	3	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	240		
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	3	240		
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	3	240		
	Prix total pour la période contractuelle un				**<À déterminer> $**

Période du contrat deux (AN. 2)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Ingénieur en sécurité de la TI	Gestion de la configuration	3	240	$	$
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	2	240	$	$
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	2	480		
Ingénieur en sécurité de la TI	PEI TS/Zonage TS	2	240		
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	3	240		
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	2	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	240		
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	3	720		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information (PEI)	3	240		

Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	3	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	240		
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	3	240		
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	3	240		
	Prix total pour la période contractuelle deux				**<À déterminer> $**

Période du contrat trois (AN. 3)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Ingénieur en sécurité de la TI	Gestion de la configuration	3	240	$	$
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	2	240	$	$
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	2	480		
Ingénieur en sécurité de la TI	PEI TS/Zonage TS	2	240		
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	3	240		
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	2	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	240		
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	3	720		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information (PEI)	3	240		

Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	3	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	240		
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	3	240		
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	3	240		
	Prix total pour la période contractuelle trois				**<À déterminer> $**

Périodes d'option :

Période d'option un (AN. 4)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Catégorie de ressources	**Titre propre à la tâche**	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme ou taux médian (s'il y a lieu)**	**Coût total (D x E)**
Ingénieur en sécurité de la TI	Gestion de la configuration	3	240	$	$
Ingénieur en sécurité de la TI	Passerelle d'échange d'information (PEI)	2	240	$	$
Ingénieur en sécurité de la TI	Architecture de référence de la cybersécurité	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Accès	3	240		
Ingénieur en sécurité de la TI	Solution interdomaines – Transfert	2	480		
Ingénieur en sécurité de la TI	PEI TS/Zonage TS	2	240		
Ingénieur en sécurité de la TI	Surveillance de la sécurité des réseaux (SSR)	3	240		
Spécialiste en conception de la sécurité de la TI	Saisie intégrale des paquets	2	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	2	240		
Spécialiste en conception de la sécurité de la TI	GIJIA et ICP	3	720		
Spécialiste en conception de la sécurité de la TI	Passerelle d'échange d'information (PEI)	3	240		

Spécialiste en conception de la sécurité de la TI	Solution interdomaines – Accès	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité des hôtes	3	240		
Spécialiste en conception de la sécurité de la TI	Sécurité réseau – Inspection du contenu	3	240		
Spécialiste en conception de la sécurité de la TI	Risque et conformité en matière de gouvernance de l'entreprise (eGRC)	3	240		
Analyste de la sécurité des réseaux	Surveillance de la sécurité des réseaux (SSR)	3	240		
Analyste de la sécurité des réseaux	SIEM (gestion de l'information de sécurité et des événements)	3	240		
Spécialiste de la gestion des incidents	SIEM (gestion de l'information de sécurité et des événements)	3	240		
	Prix total pour la période contractuelle un				**<À déterminer> $**

Prix total de la soumission :	
(Prix total de la période du contrat un + Prix total de la période du contrat deux + Prix total de la période du contrat trois + Prix total de la période d'option un)	**<À déterminer> $**

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.)

ANNEXE A – ÉNONCÉ DES TRAVAUX
VOLET DE TRAVAIL 1 – SECRET

1. CONTEXTE

1.1. L'organisation du Directeur – Ingénierie et intégration (Gestion de l'information) [DIIGI] est responsable de la conception, de la mise à l'essai et de l'intégration des capacités de l'infrastructure de gestion de l'information et de technologie de l'information (GI-TI) pour le ministère de la Défense nationale et les Forces armées canadiennes (MDN et FAC). Il soutient l'officier principal de l'information de la Défense en qualité d'ingénieur en chef et d'architecte en chef et il participe à la fonction Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance (C4ISR) et à la cybersécurité. La DIIGI détermine s'il est possible, dans l'architecture technique actuelle, d'améliorer l'efficacité, de réduire la complexité et les coûts ou d'accroître l'interopérabilité avec d'autres organismes partenaires. La section responsable de l'ingénierie relative à la cybersécurité et des services d'architecture est actuellement connue sous le nom de DIIGI 3.

1.2. La DIIGI 3 se compose de six services essentiels :

1.2.1. Orientation en matière de sécurité technique : correspond à l'élaboration, à l'interprétation ou à la mise en œuvre des normes sur la sécurité technique des TI et des processus connexes;

1.2.2. Gestion des justificatifs d'identité et de l'accès : correspond à la mise en œuvre et au renforcement des solutions d'infrastructure à clés publiques (ICP) d'entreprise du MDN et l'établissement de l'interopérabilité de l'ICP avec les autres ministères et alliés;

1.2.3. Sécurité des réseaux : correspond à la transformation de la sécurité des réseaux par l'entremise des mesures de protection, à l'intégrité et la confidentialité des transmissions des réseaux du MDN et à la sécurité du périmètre en assurant l'inspection du contenu, ainsi que la détermination, l'autorisation et l'enregistrement du trafic lorsqu'il traverse des périmètres de réseaux;

1.2.4. Sécurité des hôtes, des applications et des données : correspond au soutien en matière d'ingénierie, d'orientation et d'intégration pour mettre en œuvre des solutions de sécurité pour les hôtes validés, les applications et les données dans des environnements du MDN et des FAC;

1.2.5. Surveillance et intervention : correspond à l'ingénierie, au déploiement et au soutien des solutions techniques d'enregistrement, de vérification et de surveillance à l'appui des missions du Ministère visant la détection des cybermenaces et des utilisations malveillantes;

1.2.6. Ingénierie de la sécurité et validation : correspond à l'évaluation de la position des systèmes en matière de sécurité technique avant le volet de mise en œuvre du cycle de vie de la conception d'un système donné.

2. OBJECTIF

2.1. Le présent besoin concerne la prestation de services d'ingénierie et d'architecture de GI-TI au MDN. Les travaux exécutés dans le cadre du présent contrat permettront d'assurer le soutien de tous les systèmes et de tous les services de GI-TI des domaines classifiés et désignés liés à la cybersécurité des six services essentiels énoncés plus haut.

ANNEXE A – ÉNONCÉ DES TRAVAUX
VOLET DE TRAVAIL 1 – SECRET

3. PORTÉE

3.1. Les travaux consisteront à planifier et à mettre en œuvre de nouvelles capacités, ainsi qu'à renforcer les capacités actuelles. Toute une gamme de produits et d'équipement devra faire l'objet d'un soutien, ce qui créera des besoins variés en matière de connaissances, de compétences et d'expérience.

3.2. Les ressources travailleront principalement avec le personnel de la DIIGI du MDN. Toutefois, à certains moments, les ressources travailleront avec d'autres organisations du MDN à l'appui des initiatives visant à améliorer la sécurité des systèmes de GI-TI du MDN et des FAC.

4. DOCUMENTS PERTINENTS

4.1. Au besoin, le responsable technique (RT) fournira aux ressources les documents nécessaires pour accomplir les tâches qui leur sont attribuées. Les ressources doivent exécuter les travaux conformément aux versions approuvées par le MDN et les FAC de ces documents.

4.2. Les ressources doivent veiller à assurer la confidentialité de tous les documents et renseignements exclusifs et conserver toute la documentation en lieu sûr. Tout le matériel appartenant au MDN doit lui être remis à la fin du contrat.

5. CONTRAINTES

5.1. Les ressources doivent pouvoir travailler aux installations du MDN de la Région de la capitale nationale (RCN) de 7 h à 18 h du lundi au vendredi (à l'exception des jours fériés de la province de travail), à moins qu'il en ait été convenu autrement avec l'entrepreneur et le RT.

5.2. Tout travail effectué en dehors des heures normales de travail doit être approuvé par écrit, au préalable, par le RT. Si la personne-ressource prévoit que la journée de travail de 7,5 heures stipulée au contrat sera dépassée, elle doit obtenir l'autorisation du RT avant d'effectuer le travail au-delà de l'horaire prévu.

6. PÉRIODE DE TRANSITION

6.1. Afin d'assurer la continuité des activités, une période de transition est requise suivant l'attribution du contrat au nouvel entrepreneur pour le présent besoin. Cette période de transition laissera à ce nouvel entrepreneur le temps nécessaire pour préparer ses ressources, assumer ses responsabilités et atteindre l'état de stabilité. Elle donnera aussi à l'entrepreneur titulaire le temps de terminer ses activités en cours. Le titulaire doit transférer la responsabilité pour les activités en cours et les activités prévues à la fin de la période de transition au nouvel entrepreneur.

6.1.1. La phase de transition commence à la date d'attribution du contrat et se poursuit pendant environ deux (2) mois après l'attribution du contrat. Afin d'assurer que le niveau de service passe des services actuels d'ingénierie et d'architecture de GI-TI relatif au soutien à l'instruction et au développement des capacités aux services prévus dans l'énoncé des travaux, et ce, dans leur entièreté, et sans interruption de soutien ou perturbation des processus et opérations du MDN, l'entrepreneur devra participer aux activités suivantes :

6.1.1.1. L'entrepreneur doit fournir un plan de transition détaillé, dans les trois (3) semaines suivant l'attribution du contrat, conformément aux échéanciers convenus, pour veiller à la transition efficace de toutes les ressources et activités et permettre une préparation ordonnée et rapide afin de répondre pleinement à toutes les exigences du MDN énoncées dans le présent EDT. Le plan de transition sera élaboré en collaboration avec le MDN, puis approuvé par l'autorité technique.

6.1.1.2. Conformément au plan de transition, la transition se conclut par le transfert de responsabilité du titulaire à l'entrepreneur.

6.2. Plan de transition : L'entrepreneur devrait décrire son approche, sa méthodologie et sa gestion de l'évaluation des risques pour satisfaire aux exigences liées à la période de transition.

6.2.1 La description doit inclure au moins les éléments suivants :

a. la portée, les buts et l'objectif de la transition;
b. les activités à accomplir durant la période de transition;
c. les ressources et le niveau d'efforts requis pour accomplir chaque activité;
d. les rôles et les responsabilités du personnel clé;
e. la gestion de l'évaluation des risques;
f. les délais proposés pour toutes les activités et sous-activités et les jalons connexes.

7. TÂCHES ET PRODUITS LIVRABLES

7.1. **C.2 – Analyste des méthodes, politiques et procédures en sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Guide technique de mise en œuvre de la sécurité

L'analyste des méthodes, politiques et procédures en sécurité des TI de niveau 2 (guide technique et mise en œuvre de la sécurité) doit :

7.1.1. Créer des échéanciers et des plans de travail;
7.1.2. Fournir une orientation sur la mise en œuvre technique des différentes lignes directrices de sécurité normalisées;
7.1.3. Fournir une orientation sur le protocole Security Content Automation (SCAP);
7.1.4. Rédiger la documentation sur les politiques de sécurité et les exigences;
7.1.5. Exécuter des configurations techniques (p. ex., réalisation, conception de systèmes, guides sur le renforcement de la sécurité réseau, plans de mise à l'essai, etc.) et rédiger la documentation sur la mise en œuvre de l'ingénierie pour les nouveaux produits de sécurité;
7.1.6. Assurer la conception d'architectures de sécurité des TI et le soutien technique;

7.1.7. Rédiger des rapports techniques, comme l'analyse des possibilités et les documents d'architecture technique;

7.1.8. Fournir des conseils en matière de sécurité et produire des rapports fondés sur l'analyse des données de sécurité;

7.1.9. Fournir des éléments de réponse aux équipes de la DIIGI sur la mise en œuvre technique du renforcement de la sécurité réseau :

7.1.9.1. les hyperviseurs et les systèmes d'exploitation (p. ex, VMWare, Microsoft Windows, etc.);

7.1.9.2. les applications clients et serveurs (p. ex., les navigateurs Web, les serveurs de courriel, etc.);

7.1.9.3. les dispositifs de réseau (p. ex., les routeurs, les équilibreurs de charges, etc.).

7.1.10. Mettre en œuvre l'automatisation des essais et la validation automatisée des configurations;

7.1.11. Élaborer et mettre en œuvre des Guides de mise en œuvre technique de la sécurité (GMOTS);

7.1.12. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.1.13. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.2. **C.5 – Spécialiste de l'infrastructure à clés publiques (ICP) – Niveau 3**

Titre de la tâche précise : ICP

Le spécialiste de l'infrastructure à clés publiques (ICP) de niveau 3 doit :

7.2.1. Créer des échéanciers et des plans de travail;

7.2.2. Examiner, concevoir et élaborer des documents sur les procédés techniques liés à l'ICP, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.2.3. Examiner, analyser et intégrer les solutions d'ICP dans les services d'entreprise, y compris :

7.2.3.1. Active Directory;

7.2.3.2. les services de répertoire X.500;

7.2.3.3. la protection contre les codes malveillants axée sur l'hôte;

7.2.3.4. les services de pare-feu.

7.2.4. Élaborer et activer l'ICP avec les technologies existantes suivantes :

7.2.4.1. les pare-feu;

7.2.4.2. les courriels;

7.2.4.3. les serveurs Web;

7.2.4.4. Active Directory.

7.2.5. Conceptualiser, concevoir, élaborer, mettre à l'essai, documenter et mettre en œuvre les solutions d'ICP, entre autres : l'autorité de certification Microsoft, les modules de sécurité matériels, les solutions de gestion des cartes, les solutions de gestion de l'identité, les technologies de cartes à puce, les logiciels de carte à puce et les applications conformes à l'ICP;

7.2.6. Concevoir, mettre à l'essai, documenter et intégrer l'ICP avec des solutions de réseau privé virtuel;

7.2.7. Établir une politique de certification et des énoncés de pratique de certification applicables à l'ICP, et mener des inspections et des vérifications de la conformité à la politique;

7.2.8. Élaborer et fournir une trousse de matériel de formation pertinente à l'ICP;

7.2.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.3. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Sécurité des réseaux – Inspection du contenu

L'ingénieur en sécurité des TI de niveau 3 (sécurité des réseaux – inspection du contenu) doit :

7.3.1. Créer des échéanciers et des plans de travail;

7.3.2. Configurer et intégrer les pare-feux, et résoudre les problèmes qui y sont liés;

7.3.3. Examiner, analyser et évaluer des technologies de mandataires;

7.3.4. Configurer et intégrer l'équipement de réseau, et résoudre les problèmes qui y sont liés;

7.3.5. Analyser, mettre en œuvre et assurer la conformité aux lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information;

7.3.6. Intégrer la validation de principe des solutions de sécurité des TI dans la production;

7.3.7. Examiner, concevoir et élaborer des documents sur les procédés techniques, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de

rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.3.8. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.3.9. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.3.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.4. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Sécurité de l'hôte

Le spécialiste en conception de sécurité des TI de niveau 2 (sécurité de l'hôte) doit :

7.4.1. Créer des échéanciers et des plans de travail;

7.4.2. Évaluer les technologies liées à la sécurité de l'hôte et documenter une analyse en vue de sa gestion;

7.4.3. Concevoir, mettre sur pied, installer, configurer et mettre à l'essai les logiciels de sécurité liée à la protection des points terminaux dans un environnement d'entreprise;

7.4.4. Mettre en œuvre des politiques de sécurité aux points de terminaison axées sur l'hôte et gérées de manière centrale;

7.4.5. Appliquer les politiques de sécurité des TI et de protection des points terminaux à un système à l'échelle de l'entreprise;

7.4.6. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie;

7.4.7. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels, à la demande du RT;

7.4.8. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.4.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.5. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Passerelle d'échange d'information (PEI)

Le spécialiste en conception de sécurité des TI de niveau 3 (passerelle d'échange d'information) doit :

7.5.1. Créer des échéanciers et des plans de travail;

7.5.2. Concevoir, mettre sur pied, installer, configurer, mettre à l'essai, soutenir et tenir à jour les technologies et l'équipement de réseautage liés à la sécurité suivants :

- 7.5.2.1. les sentinelles et passerelles;
- 7.5.2.2. les pare-feu;
- 7.5.2.3. les services de protection des limites de réseau;
- 7.5.2.4. les diodes de données;
- 7.5.2.5. les mandataires Web;
- 7.5.2.6. les agents de transfert de courriel.

7.5.3. Concevoir, mettre sur pied, installer, configurer, mettre à l'essai, soutenir et tenir à jour les produits et infrastructures de TI suivants, et résoudre les problèmes qui y sont liés :

- 7.5.3.1. le système d'exploitation en réseau Microsoft;
- 7.5.3.2. les réseaux IP;
- 7.5.3.3. l'intégration des applications;
- 7.5.3.4. la virtualisation.

7.5.4. Examiner, concevoir et élaborer des documents sur les procédés techniques, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.5.5. Configurer, intégrer et fournir l'équipement et les technologies de réseautage;

7.5.6. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.5.7. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.5.8. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.6. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Sécurité des réseaux – Inspection du contenu

Le spécialiste en conception de sécurité des TI de niveau 3 (sécurité des réseaux – inspection du contenu) doit :

7.6.1. Créer des échéanciers et des plans de travail;

7.6.2. Configurer, intégrer et fournir des équilibreurs de charges des réseaux;

7.6.3. Examiner, analyser et évaluer les systèmes de détection des intrusions, les générateurs d'achalandage orientés vers les applications et les technologies de chiffrement;

7.6.4. Configurer et intégrer les pare-feux, et résoudre les problèmes qui y sont liés;

7.6.5. Configurer et intégrer l'équipement de réseau, et résoudre les problèmes qui y sont liés;

7.6.6. Analyser, mettre en œuvre et assurer la conformité, sur les réseaux pris en charge, aux lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information publiées par le Centre de la sécurité des télécommunications (CSE);

7.6.7. Intégrer la validation de principe des solutions de sécurité des TI dans la production;

7.6.8. Examiner, concevoir et élaborer des documents sur les procédés techniques, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.6.9. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.6.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.6.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.7. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Sécurité de la virtualisation

Le spécialiste en conception de sécurité des TI de niveau 3 (sécurité de la virtualisation) doit :

7.7.1. Préparer des horaires et des plans de travail;

7.7.2. Configurer, intégrer et mettre en œuvre les technologies de virtualisation;

7.7.3. Concevoir les solutions d'infrastructure de bureau virtuel (IBV);

7.7.4. Examiner, concevoir et élaborer des documents sur les procédés techniques, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de

rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.7.5. Analyser, mettre en œuvre et assurer la conformité, sur les réseaux pris en charge, aux lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information publiées par le Centre de la sécurité des télécommunications (CSE);

7.7.6. Fournir une orientation pour sécuriser de façon appropriée les infrastructures virtualisées;

7.7.7. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.7.8. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.7.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.8. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Soutien en service du Système national de protection des terminaux (NEPS ISS)

Le spécialiste en conception de sécurité des TI de niveau 3 (soutien en service du Système national de protection des terminaux) doit :

7.8.1. Préparer des horaires et des plans de travail;

7.8.2. Concevoir, développer, mettre à l'essai et mettre en œuvre le logiciel Stormshield Endpoint Security (version 7.x ou plus récente) dans un environnement d'entreprise;

7.8.3. Concevoir, développer, mettre à l'essai et mettre en œuvre la solution de sécurité Symantec Enterprise Protection (version 12.x ou plus récente) dans un environnement d'entreprise;

7.8.4. Analyser les outils et les techniques Endpoint Security et documenter les menaces potentielles à la sécurité des TI relativement aux systèmes de la DIIGI;

7.8.5. Examiner les registres de sécurité détaillés et l'utilisateur de la sécurité en vue de fournir une analyse des tendances, des conseils ainsi que des rapports sur les menaces potentielles à la sécurité des TI;

7.8.6. Analyser les statistiques des TI;

7.8.7. Préparer des rapports techniques, comme l'analyse des besoins, l'analyse des possibilités, les documents d'architecture technique, etc.;

7.8.8. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.8.9. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.8.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.9. **C.8 – Analyste de la sécurité des réseaux – Niveau 2**

Titre de la tâche précise : Soutien en service du Système national de protection des terminaux (NEPS ISS)

L'analyste de la sécurité des réseaux de niveau 2 (soutien en service du Système national de protection des terminaux) doit :

7.9.1. Préparer des horaires et des plans de travail;

7.9.2. Soutenir et tenir à jour le logiciel de sécurité Symantec Endpoint Protection (version 12.x ou plus récente) dans un environnement d'entreprise;

7.9.3. Soutenir et tenir à jour le logiciel de McAfee ePolicy Orchestrator dans un environnement d'entreprise;

7.9.4. Soutenir et tenir à jour le logiciel de sécurité Stormshield Endpoint Security (version 7.x ou plus récente) dans un environnement d'entreprise;

7.9.5. Mettre en œuvre et tenir à jour les politiques de pare-feu axées sur l'hôte relatives aux serveurs de protection des points terminaux;

7.9.6. Mettre en œuvre et tenir à jour les règles des systèmes de prévention des intrusions axées sur l'hôte (HIPS) relatives aux serveurs de protection des points terminaux;

7.9.7. Mettre en œuvre, encoder et tenir à jour les iRules BIG-IP F5;

7.9.8. Configurer et soutenir les différents logiciels de sécurité des points terminaux pris en charge par Microsoft Windows 7, Windows 10, Windows Server 2008, ou Windows Server 2012;

7.9.9. Installer, sauvegarder et restaurer les bases de données Microsoft Search and Query Language (SQL) et offrir un service de réparation de bris;

7.9.10. Soutenir et tenir à jour les serveurs Syslog;

7.9.11. Déceler et analyser les menaces techniques pesant sur les réseaux et les vulnérabilités de ces derniers;

7.9.12. Analyser les répercussions de la sécurité des réseaux pour la mise en œuvre de nouveaux logiciels et de modifications de configuration importantes ainsi que pour la gestion des correctifs;

7.9.13. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.9.14. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.10. **C.8 – Analyste de la sécurité des réseaux – Niveau 2**

Titre de la tâche précise : Passerelle d'échange d'information (PEI)

L'analyste de la sécurité des réseaux de niveau 2 (passerelle d'échange d'information) doit :

7.10.1. Préparer des horaires et des plans de travail;

7.10.2. Concevoir, mettre sur pied, installer, configurer, mettre à l'essai, soutenir et tenir à jour les technologies et l'équipement de réseautage liés à la sécurité suivants :

7.10.2.1. les pare-feu;

7.10.2.2. les mandataires Web;

7.10.2.3. les agents de transfert de courriel.

7.10.3. Examiner, concevoir et élaborer des documents sur les procédés techniques, entre autres : des documents sur les exigences, les architectures des solutions, la réalisation et la configuration; des plans de mise à l'essai; des procédures opérationnelles normalisées (PON); des guides de l'utilisateur; des mesures de rendement des systèmes et de la planification de la capacité et des documents sur la planification de la continuité des opérations et de la reprise des activités;

7.10.4. Configurer et intégrer l'équipement et les technologies de réseautage, y compris mettre en œuvre des protocoles dynamiques de routage;

7.10.5. Configurer, intégrer et mettre en œuvre les technologies de réseaux IP;

7.10.6. Configurer, intégrer et mettre en œuvre Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine;

7.10.7. Concevoir et configurer la distribution du trafic d'applications au moyen d'équilibreurs de charges;

7.10.8. Configurer, intégrer et mettre en œuvre les technologies de virtualisation;

7.10.9. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.10.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.10.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.11. **C.8 – Analyste de la sécurité des réseaux – Niveau 3**

Titre de la tâche précise : Surveillance de la sécurité des réseaux

L'analyste de la sécurité des réseaux de niveau 3 (surveillance de la sécurité des réseaux) doit :

7.11.1. Préparer des horaires et des plans de travail;

7.11.2. Assurer la détection et l'analyse des incidents liés à la sécurité des TI, ainsi que les services de traitement connexes;

7.11.3. Surveiller et analyser les fichiers des journaux de sécurité pour les menaces à la sécurité des TI;

7.11.4. Surveiller, configurer, mettre au point et optimiser les outils de gestion des événements et des informations de sécurité (SIEM) ou de capture complète des paquets;

7.11.5. Examiner, élaborer et mettre en œuvre les flux des processus d'acheminement des problèmes et de traitement des incidents;

7.11.6. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels à la demande du RT;

7.11.7. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

8. EXIGENCES EN MATIÈRE DE RAPPORTS

8.1. L'entrepreneur doit présenter un rapport de progression mensuel pour chacune des ressources et l'envoyer au RT au début du mois suivant. Une copie de ce rapport doit également être jointe à la facture mensuelle. Chacun de ces rapports doit contenir au moins les renseignements suivants :

8.1.1. toutes les activités importantes réalisées au cours de la période visée susceptibles d'avoir une incidence sur le rendement des travaux;

8.1.2. l'état de toute activité non terminée qui peut dépasser les délais normaux;

8.1.3. la description des problèmes rencontrés qui nécessiteront une attention ou qui pourraient s'aggraver; et

8.1.4. des recommandations visant à mettre à jour les procédures.

8.2. Tous les rapports doivent être remis dans un format acceptable aux yeux du RT.

9. EXIGENCES LINGUISTIQUES

9.1. Chacune des autorisations de tâches précisera les exigences linguistiques.

9.1.1. Les ressources doivent maîtriser l'anglais pour toutes les tâches. Par « maîtriser », on entend la capacité à communiquer de vive voix ou par écrit, sans aide et en faisant peu d'erreurs.

10. LIEU DE TRAVAIL

10.1. Tous les travaux doivent être accomplis dans les installations du MDN au sein de la RCN.

11. DÉPLACEMENTS

11.1. Les frais de déplacement au sein de la RCN ne seront pas remboursés.

11.2. Si, pendant la période du contrat, des déplacements s'avèrent nécessaires à l'extérieur de la RCN, les factures de frais de déplacement et de subsistance présentées doivent être accompagnées de pièces justificatives (reçus) et seront remboursées conformément à la politique et aux lignes directrices du Conseil du Trésor sur les voyages en vigueur au moment des déplacements, au coût réel, sans provision pour la marge bénéficiaire ou le profit. Tous les déplacements à l'extérieur de la RCN doivent être approuvés au préalable par le RT par écrit.

ANNEXE A – ÉNONCÉ DES TRAVAUX
VOLET DE TRAVAIL 2 – TRÈS SECRET

1. CONTEXTE

1.1. L'organisation du Directeur – Ingénierie et intégration (Gestion de l'information) [DIIGI] est responsable de la conception, de la mise à l'essai et de l'intégration des capacités de l'infrastructure de gestion de l'information et de technologie de l'information (GI-TI) pour le ministère de la Défense nationale et les Forces armées canadiennes (MDN et FAC). Il soutient l'officier principal de l'information de la Défense en qualité d'ingénieur en chef et d'architecte en chef et il participe à la fonction Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance (C4ISR) et à la cybersécurité. La DIIGI détermine s'il est possible, dans l'architecture technique actuelle, d'améliorer l'efficacité, de réduire la complexité et les coûts ou d'accroître l'interopérabilité avec d'autres organismes partenaires. La section responsable de l'ingénierie relative à la cybersécurité et des services d'architecture est actuellement connue sous le nom de DIIGI 3.

1.2. La DIIGI 3 se compose de six services essentiels :

1.2.1. Orientation en matière de sécurité technique : correspond à l'élaboration, à l'interprétation ou à la mise en œuvre des normes sur la sécurité technique des TI et des processus connexes;

1.2.2. Gestion des justificatifs d'identité et de l'accès : correspond à la mise en œuvre et au renforcement des solutions d'infrastructure à clés publiques (ICP) d'entreprise du MDN et l'établissement de l'interopérabilité de l'ICP avec les autres ministères et alliés;

1.2.3. Sécurité des réseaux : correspond à la transformation de la sécurité des réseaux par l'entremise des mesures de protection, à l'intégrité et la confidentialité des transmissions des réseaux du MDN et à la sécurité du périmètre en assurant l'inspection du contenu, ainsi que la détermination, l'autorisation et l'enregistrement du trafic lorsqu'il traverse des périmètres de réseaux;

1.2.4. Sécurité des hôtes, des applications et des données : correspond au soutien en matière d'ingénierie, d'orientation et d'intégration pour mettre en œuvre des solutions de sécurité pour les hôtes validés, les applications et les données dans des environnements du MDN et des FAC;

1.2.5. Surveillance et intervention : correspond à l'ingénierie, au déploiement et au soutien des solutions techniques d'enregistrement, de vérification et de surveillance à l'appui des missions du Ministère visant la détection des cybermenaces et des utilisations malveillantes;

1.2.6. Ingénierie de la sécurité et validation : correspond à l'évaluation de la position des systèmes en matière de sécurité technique avant le volet de mise en œuvre du cycle de vie de la conception d'un système donné.

2. OBJECTIF

2.1. Le présent besoin concerne la prestation de services d'ingénierie et d'architecture de GI-TI au MDN. Les travaux exécutés dans le cadre du présent contrat permettront d'assurer le soutien de tous les systèmes et de tous les services de GI-TI des domaines classifiés et désignés liés à la cybersécurité des six services essentiels énoncés plus haut.

ANNEXE A – ÉNONCÉ DES TRAVAUX
VOLET DE TRAVAIL 2 – TRÈS SECRET

3. PORTÉE

3.1. Les travaux consisteront à planifier et à mettre en œuvre de nouvelles capacités, ainsi qu'à renforcer les capacités actuelles. Toute une gamme de produits et d'équipement devra faire l'objet d'un soutien, ce qui créera des besoins variés en matière de connaissances, de compétences et d'expérience.

3.2. Les ressources travailleront principalement avec le personnel de la DIIGI du MDN. Toutefois, à certains moments, les ressources travailleront avec d'autres organisations du MDN à l'appui des initiatives visant à améliorer la sécurité des systèmes de GI-TI du MDN et des FAC.

4. DOCUMENTS PERTINENTS

4.1. Au besoin, le responsable technique (RT) fournira aux ressources les documents nécessaires pour accomplir les tâches qui leur sont attribuées. Les ressources doivent exécuter les travaux conformément aux versions approuvées par le MDN et les FAC de ces documents.

4.2. Les ressources doivent veiller à assurer la confidentialité de tous les documents et renseignements exclusifs et conserver toute la documentation en lieu sûr. Tout le matériel appartenant au MDN doit lui être remis à la fin du contrat.

5. CONTRAINTES

5.1. Les ressources doivent pouvoir travailler aux installations du MDN de la Région de la capitale nationale (RCN) de 7 h à 18 h du lundi au vendredi (à l'exception des jours fériés de la province de travail), à moins qu'il en ait été convenu autrement avec l'entrepreneur et le RT.

5.2. Tout travail effectué en dehors des heures normales de travail doit être approuvé par écrit au préalable par le RT. Si la personne-ressource prévoit que la journée de travail de 7,5 heures stipulée au contrat sera dépassée, elle doit obtenir l'autorisation du RT avant d'effectuer le travail au-delà de l'horaire prévu.

6. PÉRIODE DE TRANSITION

6.1. Afin d'assurer la continuité des activités, une période de transition est requise suivant l'attribution du contrat au nouvel entrepreneur pour le présent besoin. Cette période de transition laissera à ce nouvel entrepreneur le temps nécessaire pour préparer ses ressources, assumer ses responsabilités et atteindre l'état de stabilité. Elle donnera aussi à l'entrepreneur titulaire le temps de terminer ses activités en cours. Le titulaire doit transférer la responsabilité pour les activités en cours et les activités prévues à la fin de la période de transition au nouvel entrepreneur.

6.1.1. La phase de transition commence à la date d'attribution du contrat et se poursuit pendant environ deux (2) mois après l'attribution du contrat. Afin d'assurer que le niveau de service passe des services actuels d'ingénierie et d'architecture de GI-TI relatif au soutien à l'instruction et au développement des capacités aux services prévus dans l'énoncé des travaux, et ce, dans leur entièreté, et sans interruption de soutien ou perturbation des processus et opérations du MDN, l'entrepreneur devra s'acquitter de ce qui suit :

6.1.1.1. L'entrepreneur doit fournir un plan de transition détaillé, dans les trois (3) semaines suivant l'attribution du contrat, conformément aux

échéanciers convenus, pour veiller à la transition efficace de toutes les ressources et activités et permettre une préparation ordonnée et rapide afin de répondre pleinement à toutes les exigences du MDN énoncées dans le présent EDT. Le plan de transition sera élaboré en collaboration avec le MDN, puis approuvé par l'autorité technique.

6.1.1.2. Conformément au plan de transition, la transition se conclut par le transfert de responsabilité du titulaire à l'entrepreneur.

6.2. Plan de transition : L'entrepreneur devrait décrire son approche, sa méthodologie et sa gestion de l'évaluation des risques pour satisfaire aux exigences liées à la période de transition.

6.2.1 La description doit inclure au moins les éléments suivants :

a. La portée, les buts et l'objectif de la transition;
b. les activités à accomplir durant la période de transition;
c. les ressources et le niveau d'efforts requis pour accomplir chaque activité;
d. les rôles et les responsabilités du personnel clé;
e. la gestion de l'évaluation des risques;
f. les délais proposés pour toutes les activités et sous-activités et les jalons connexes.

7. TÂCHES ET PRODUITS LIVRABLES

7.1. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Gestion de la configuration

L'ingénieur en sécurité des TI de niveau 3 (gestion de la configuration) doit :

7.1.1. Créer des échéanciers et des plans de travail;
7.1.2. Planifier et mettre en œuvre des solutions de sécurité des TI pour les environnements de réseau du MDN;
7.1.3. Assurer la conception d'architectures de sécurité des TI et le soutien technique;
7.1.4. Planifier, élaborer, mettre en œuvre et intégrer les solutions d'évaluation de la vulnérabilité;
7.1.5. Élaborer et mettre en œuvre un programme de gestion de la vulnérabilité pour une grande organisation du MDN;
7.1.6. Fournir une analyse des options des outils et des techniques de sécurité de TI les plus récents;
7.1.7. Exécuter une analyse des données de sécurité (p. ex., le suivi des événements, la découverte d'actifs, les risques de menace, les rapports d'incident, etc.) et fournir des avis et des rapports;
7.1.8. Planifier, élaborer, mettre en œuvre et intégrer les solutions de découverte d'actifs et de bases de données de gestion des configurations (BDGC) de TI;

7.1.9. Planifier, élaborer, mettre en œuvre et intégrer les solutions de vérification automatisée de la conformité de la configuration;

7.1.10. Examiner, concevoir et élaborer des rapports sur les procédés techniques, entre autres : une analyse des besoins, des guides sur le renforcement de la sécurité réseau et des documents d'architecture technique;

7.1.11. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.1.12. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.1.13. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.2. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Passerelle d'échange d'information (PEI)

L'ingénieur en sécurité des technologies de l'information de niveau 2 (passerelle d'échange d'information) doit :

7.2.1. Créer des échéanciers et des plans de travail;

7.2.2. Mettre sur pied, concevoir, configurer, intégrer et mettre en œuvre :

7.2.2.1. des solutions de pare-feu;

7.2.2.2. des solutions de mandataire Web;

7.2.2.3. des solutions de transfert de courrier;

7.2.2.4. des solutions de service de protection des limites de réseau;

7.2.2.5. des solutions SSL, HTTPS, HTTP, IPSec et SMTP;

7.2.2.6. des solutions de virtualisation;

7.2.2.7. le répertoire actif et le système de noms de domaine de Windows 2008 (ou version plus récente).

7.2.3. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.2.4. Mettre sur pied, configurer, intégrer et fournir des technologies de réseautage;

7.2.5. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.2.6. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.2.7. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) à l'appui du programme ministériel de cyberprotection et de sécurité des TI.

7.3. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Architecture de référence de cybersécurité

L'ingénieur en sécurité des TI de niveau 3 (architecture de référence de cybersécurité) doit :

7.3.1. Créer des échéanciers et des plans de travail;

7.3.2. Examiner, recenser, analyser, concevoir, mettre en œuvre et gérer les architectures de sécurité des TI;

7.3.3. Appliquer les processus de gestion des risques liés à la sécurité des TI;

7.3.4. Concevoir, mettre en œuvre et configurer les méthodes de protection et de détection des intrusions des TI;

7.3.5. Concevoir, mettre en œuvre et configurer la surveillance des systèmes;

7.3.6. Concevoir, mettre en œuvre et configurer les services de TI d'entreprise, notamment le répertoire, l'identification unique, le courriel, la sauvegarde ou la base de données répartie;

7.3.7. Concevoir, mettre en œuvre et configurer les principes de défense en profondeur des TI;

7.3.8. Élaborer des rapports techniques et des documents d'ingénierie, entre autres : une analyse des besoins, des documents sur la configuration et des documents d'architecture technique;

7.3.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.3.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.3.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.4. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Solution transectorielle – Accès

L'ingénieur en sécurité des TI de niveau 3 (solution transectorielle – accès) doit :

7.4.1. Créer des échéanciers et des plans de travail;

7.4.2. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.4.3. Configurer, intégrer et mettre en œuvre Microsoft Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine;

7.4.4. Concevoir et mettre en œuvre des contrôles et des politiques liées à la sécurité des réseaux;

7.4.5. Configurer et intégrer des technologies de pare-feu;

7.4.6. Concevoir et offrir des services de bureau virtuel;

7.4.7. Concevoir, configurer et mettre en œuvre des technologies de réseautage et veiller à la gestion du changement;

7.4.8. Concevoir, configurer et mettre en œuvre des modèles de contrôle d'accès en fonction des rôles et reposant sur des règles;

7.4.9. Concevoir, configurer et mettre en œuvre des schémas de tunnellisation d'IPsec;

7.4.10. Analyser, configurer, intégrer et mettre en œuvre diverses technologies de la sécurité y compris, mais sans s'y limiter :

7.4.10.1. les normes de répertoire, comme le protocole SMTP;

7.4.10.2. les protocoles réseau comme HTTP, FTP et Telnet;

7.4.10.3. les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, SSL, TSL, SMTP et SSH.

7.4.11. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.4.12. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels, à la demande du RT;

7.4.13. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.4.14. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.5. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Solution transectorielle – Transfert

L'ingénieur en sécurité des TI de niveau 2 (solution transectorielle – transfert) doit :

7.5.1. Créer des échéanciers et des plans de travail;

7.5.2. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.5.3. Configurer, intégrer et mettre en œuvre Microsoft Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine;

7.5.4. Configurer et intégrer ce qui suit :

7.5.4.1. les technologies de protection de niveau d'assurance élevé;

7.5.4.2. les technologies de pare-feu;

7.5.4.3. les technologies de transfert de courrier.

7.5.5. Mettre sur pied, concevoir, configurer et intégrer des solutions de filtrage de contenu de courriel et de prévention des pertes de données, et des solutions virtualisées;

7.5.6. Analyser, configurer, intégrer et mettre en œuvre diverses technologies de la sécurité y compris, mais sans s'y limiter :

7.5.6.1. les normes de répertoire, comme le protocole SMTP;

7.5.6.2. les protocoles réseau comme HTTP, FTP et Telnet;

7.5.6.3. les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, SSL, TSL, SMTP et SSH.

7.5.7. Mettre sur pied, configurer, intégrer et fournir des technologies de réseautage;

7.5.8. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.5.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.5.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.5.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.6. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Passerelle d'échange d'information (PEI) et zonage

L'ingénieur en sécurité des TI de niveau 2 (passerelle d'échange d'information et zonage) doit :

7.6.1. Créer des échéanciers et des plans de travail;

7.6.2. Configurer et intégrer ce qui suit :

7.6.2.1. les technologies de pare-feu;

7.6.2.2. les technologies de mandataire Web;

7.6.2.3. les technologies de transfert de courrier;

7.6.2.4. des solutions de service de protection des limites de réseau.

7.6.3. Mettre sur pied, configurer, intégrer et mettre en œuvre diverses technologies de la sécurité, y compris, mais sans s'y limiter :

7.6.3.1. les normes de répertoire, comme le protocole SMTP;

7.6.3.2. les protocoles réseau comme HTTP, FTP et Telnet;

7.6.3.3. les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, SSL, TSL, SMTP et SSH.

7.6.4. Mettre sur pied, configurer, intégrer et mettre en œuvre Microsoft Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine;

7.6.5. Mettre sur pied, configurer et intégrer des solutions de filtrage de contenu de courriel et de prévention des pertes de données, et des solutions virtualisées;

7.6.6. Mettre sur pied, configurer, intégrer et fournir des technologies de réseautage;

7.6.7. Concevoir des solutions de surveillance de la sécurité des réseaux en fonction des lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information;

7.6.8. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.6.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.6.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.6.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.7. **C.6 – Ingénieur en sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Surveillance de la sécurité des réseaux

L'ingénieur en sécurité des TI de niveau 3 (surveillance de la sécurité des réseaux) doit :

7.7.1. Créer des échéanciers et des plans de travail;

7.7.2. Composer et tenir à jour les documents techniques sur la gestion des événements et des informations de sécurité (SIEM) ou sur la capture complète des paquets;

7.7.3. Concevoir des solutions de surveillance de la sécurité des réseaux en fonction des lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information;

7.7.4. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.7.5. Concevoir, déployer et intégrer des outils de gestion des événements et des informations de sécurité (SIEM) dans un environnement de production;

7.7.6. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.7.7. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;

7.7.8. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.8. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Capture complète des paquets

Le spécialiste en conception de sécurité des TI de niveau 2 (capture complète des paquets) doit :

7.8.1. Créer des échéanciers et des plans de travail;

7.8.2. Concevoir, déployer et administrer les composants d'infrastructure de communication du réseau local et étendu et résoudre les problèmes liés à celui-ci;

7.8.3. Administrer Linux (ou une variante de Linux);

7.8.4. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.8.5. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.8.6. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.8.7. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.9. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 2**

Titre de la tâche précise : Sécurité de l'hôte

Le spécialiste en conception de sécurité des TI de niveau 2 (sécurité de l'hôte) doit :

7.9.1. Créer des échéanciers et des plans de travail;

7.9.2. Évaluer les technologies liées à la sécurité de l'hôte et fournir une analyse détaillée en vue de sa gestion;

7.9.3. Concevoir, mettre sur pied, installer, configurer et mettre à l'essai les logiciels de sécurité liée à la protection des points terminaux dans un environnement d'entreprise;

7.9.4. Mettre en œuvre des politiques de sécurité aux points de terminaison axées sur l'hôte et gérées de manière centrale;

7.9.5. Appliquer les politiques de sécurité des TI et de protection des points terminaux à un système à l'échelle de l'entreprise;

7.9.6. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.9.7. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.9.8. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.9.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.10. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et infrastructure à clés publiques (ICP)

Le spécialiste en conception de sécurité des TI de niveau 3 (gestion de l'identité, des justificatifs d'identité et de l'accès et infrastructure à clés publiques) doit :

7.10.1. Créer des échéanciers et des plans de travail;

7.10.2. Examiner, analyser et appliquer : des méthodes, modèles et cadres d'architecture comme TOGAF, FEAP (gouvernement américain), BTEP (gouvernement canadien), Zachman, le cadre SABSA, etc.;

7.10.3. Examiner, analyser et appliquer :

7.10.3.1. les architectures et normes de sécurité des TI;

7.10.3.2. les technologies et les tendances du marché;

7.10.3.3. les pratiques exemplaires et les normes.

7.10.4. Produire et tenir des réunions d'information sur les menaces, les répercussions, les vulnérabilités ou les risques liés à la sécurité des TI à l'intention des cadres supérieurs;

7.10.5. Analyser, concevoir et établir l'interopérabilité de l'ICP avec les autres ministères et alliés;

7.10.6. Analyser et élaborer la conception des exigences en matière d'architecture GIJIA et ICP, ainsi que la mise en œuvre et la schématisation des processus;

7.10.7. Prendre en charge les processus d'évaluation de la sécurité et l'autorisation (ESA);

7.10.8. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les procédures normales d'exploitation (PNE), le concept des opérations, les plans de mise en œuvre de systèmes, les plans de soutien du cycle de vie;

7.10.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.10.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.10.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.11. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Passerelle d'échange d'information (PEI)

Le spécialiste en conception de sécurité des TI de niveau 3 (passerelle d'échange d'information) doit :

7.11.1. Créer des échéanciers et des plans de travail;

7.11.2. Concevoir, mettre sur pied, installer, configurer, mettre à l'essai, soutenir et tenir à jour les produits de TI suivants :

- 7.11.2.1. les sentinelles et passerelles;
- 7.11.2.2. les pare-feux;
- 7.11.2.3. les services de protection des limites de réseau;
- 7.11.2.4. les diodes de données;
- 7.11.2.5. les mandataires Web;
- 7.11.2.6. les agents de transfert de courrier;
- 7.11.2.7. les systèmes d'exploitation en réseau Microsoft;
- 7.11.2.8. les réseaux IP;
- 7.11.2.9. l'intégration des applications;
- 7.11.2.10. la virtualisation.

7.11.3. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.11.4. Configurer, intégrer et fournir des technologies de réseautage, y compris des routeurs et commutateurs;

7.11.5. Analyser, configurer, intégrer et mettre en œuvre diverses technologies de la sécurité y compris, mais sans s'y limiter :

- 7.11.5.1. les normes de répertoire, comme le protocole SMTP;
- 7.11.5.2. les protocoles réseau comme HTTP, FTP et Telnet;
- 7.11.5.3. les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, SSL, TSL, SMTP et SSH.

7.11.6. Configurer, intégrer et mettre en œuvre Microsoft Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine dans un système à l'échelle de l'entreprise;

7.11.7. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.11.8. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.11.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.12. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Solution transectorielle – Accès

Le spécialiste en conception de sécurité des TI de niveau 3 (solution transectorielle – accès) doit :

7.12.1. Créer des échéanciers et des plans de travail;

7.12.2. Examiner, analyser et appliquer des méthodes, modèles et cadres d'architecture comme TOGAF, FEAP (gouvernement américain), BTEP (gouvernement canadien), GSRM, Zachman, etc.;

7.12.3. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.12.4. Préparer des rapports techniques pour les solutions transectorielles, comme l'analyse des besoins, l'analyse des possibilités, les documents d'architecture technique, la modélisation mathématique des risques, etc.;

7.12.5. Configurer, intégrer et mettre en œuvre Microsoft Windows 2008 Server (ou une version plus récente), le Répertoire actif et le Système de noms de domaine;

7.12.6. Exécuter la mise en œuvre de la conception et la gestion du changement des contrôles et politiques liées à la sécurité des réseaux;

7.12.7. Exécuter la mise en œuvre de la conception et la gestion du changement des services de bureau virtuel;

7.12.8. Exécuter la mise en œuvre de la conception et la gestion du changement des technologies de réseautage;

7.12.9. Exécuter la mise en œuvre de la conception et la gestion du changement des modèles de contrôle d'accès en fonction des rôles et reposant sur des règles;

7.12.10. Exécuter la mise en œuvre de la conception et la gestion du changement des schémas de tunnellisation IPSec;

7.12.11. Analyser les outils et les techniques de sécurité des TI liés aux solutions transectorielles;

7.12.12. Analyser les données de sécurité et présenter des avis et des rapports liés aux solutions transectorielles;

7.12.13. Assurer la conception d'architectures de sécurité des TI et le soutien technique;

7.12.14. Réaliser des études liées à la classification de sécurité des données;

7.12.15. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.12.16. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.12.17. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.13. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Sécurité de l'hôte

Le spécialiste en conception de sécurité des TI de niveau 3 (sécurité de l'hôte) doit :

7.13.1. Créer des échéanciers et des plans de travail;

7.13.2. Évaluer les technologies liées à la sécurité de l'hôte et fournir une analyse détaillée en vue de sa gestion;

7.13.3. Concevoir, mettre sur pied, installer, configurer et mettre à l'essai les logiciels de sécurité liée à la protection des points terminaux dans un environnement d'entreprise;

7.13.4. Mettre en œuvre des politiques de sécurité aux points de terminaison axées sur l'hôte et gérées de manière centrale;

7.13.5. Appliquer les politiques de sécurité des TI et de protection des points terminaux à un système à l'échelle de l'entreprise;

7.13.6. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.13.7. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.13.8. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.13.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.14. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Sécurité des réseaux – Inspection du contenu

Le spécialiste en conception de sécurité des TI de niveau 3 (sécurité des réseaux – inspection du contenu) doit :

7.14.1. Créer des échéanciers et des plans de travail;

7.14.2. Examiner, analyser les politiques de sécurité des TI ainsi que les lignes directrices en matière de contrôle de sécurité et de zonage fédérales, provinciales et territoriales, et s'assurer que le MDN s'y conforme;

7.14.3. Intégrer la validation de principe des solutions de sécurité des TI dans un environnement de production;

7.14.4. Configurer, intégrer et tenir à jour les pare-feux dans un environnement de production, et résoudre les problèmes qui y sont liés;

7.14.5. Configurer, intégrer et fournir des technologies de réseautage;

7.14.6. Configurer, intégrer et tenir à jour la technologie de virtualisation;

7.14.7. Configurer et surveiller des systèmes de détection d'intrusion;

7.14.8. Configurer, intégrer et fournir des équilibreurs de charges;

7.14.9. Participer aux réunions et aux groupes de travail hebdomadaires ou bimensuels, à la demande du RT;

7.14.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.14.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.15. **C.7 – Spécialiste en conception de sécurité des technologies de l'information – Niveau 3**

Titre de la tâche précise : Gouvernance, risque et conformité de l'entreprise

Le spécialiste en conception de sécurité des TI de niveau 3 (gouvernance, risque et conformité de l'entreprise) doit :

7.15.1. Créer des échéanciers et des plans de travail;

7.15.2. Élaborer et mettre en œuvre un programme de gouvernance, de risque et de conformité de l'entreprise;

7.15.3. Évaluer l'application de contrôles de sécurité, évaluer les menaces et les risques associés à un système de TI et interpréter et appliquer les Conseils en matière de sécurité des technologies de l'information (ITSG) 33;

7.15.4. Définir et mettre en œuvre les différentes étapes d'un projet de sécurité des TI, comme définir les besoins, les solutions d'ingénierie, etc.;

7.15.5. Examiner, concevoir et élaborer des documents sur les procédés techniques comme les spécifications de la conception du système, les documents sur la réalisation et la configuration, le concept des opérations, les plans de mise en œuvre de systèmes, les plans de mise à l'essai, les rapports de mise à l'essai, les plans de soutien du cycle de vie, etc.;

7.15.6. Examiner les processus d'évaluation de la sécurité et l'autorisation (ESA);

7.15.7. Analyser et fournir des rapports sur la conception d'architecture de sécurité des TI;

7.15.8. Concevoir des solutions de surveillance de la sécurité des réseaux en fonction des lignes directrices en matière de contrôle de sécurité et de zonage des Conseils en matière de sécurité des technologies de l'information;

7.15.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.15.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.15.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.16. **C.8 – Analyste de la sécurité des réseaux – Niveau 3**

Titre de la tâche précise : Surveillance de la sécurité des réseaux

L'analyste de la sécurité des réseaux de niveau 3 (surveillance de la sécurité des réseaux) doit :

7.16.1. Créer des échéanciers et des plans de travail;

7.16.2. Surveiller et analyser les fichiers des journaux de sécurité;

7.16.3. Recueillir et analyser les codes malveillants auprès des hôtes et du trafic réseau;

7.16.4. Surveiller, configurer et affiner les outils de gestion des événements et des informations de sécurité (SIEM) ou de capture complète des paquets;

7.16.5. Exécuter la surveillance de la sécurité des réseaux et faire une analyse des journaux afin de détecter les activités malveillantes;

7.16.6. Assurer la détection et l'analyse des incidents liés à la sécurité des TI, ainsi que les services de traitement connexes au moyen d'outils SIEM automatisés;

7.16.7. Exploiter et configurer tous les aspects d'une solution SIEM;

7.16.8. Examiner, élaborer et mettre en œuvre les flux des processus d'acheminement des problèmes et de traitement des incidents;

7.16.9. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.16.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.17. **C.8 – Analyste de la sécurité des réseaux – Niveau 3**

Titre de la tâche précise : Gestion des événements et des informations de sécurité (SIEM)

L'analyste de la sécurité des réseaux de niveau 3 (gestion des événements et des informations de sécurité) doit :

7.17.1. Créer des échéanciers et des plans de travail;

7.17.2. Surveiller et analyser les fichiers des journaux de sécurité;

7.17.3. Concevoir et mettre en œuvre des cas d'utilisation de la SIEM pour les serveurs et les postes;

7.17.4. Bâtir et configurer les serveurs Linux et résoudre les problèmes liés à ceux-ci;

7.17.5. Configurer et fournir un soutien technique à l'outil logiciel commercial ArcSight;

7.17.6. Déployer et exploiter tous les aspects d'une solution SIEM;

7.17.7. Exécuter la surveillance de la sécurité des réseaux et faire une analyse des journaux afin de détecter les activités malveillantes;

7.17.8. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.17.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

7.18. **C.12 – Spécialiste de la gestion des incidents – Niveau 3**

Titre de la tâche précise : Gestion des événements et des informations de sécurité (SIEM)

Le spécialiste de la gestion des incidents de niveau 3 (gestion des événements et des informations de sécurité) doit :

7.18.1. Créer des échéanciers et des plans de travail;

7.18.2. Mettre en œuvre et fournir un soutien technique pour l'outil logiciel commercial ArcSight;

7.18.3. Concevoir et mettre en œuvre des cas d'utilisation de la SIEM pour les serveurs et les postes;

7.18.4. Bâtir et configurer les serveurs Linux et résoudre les problèmes liés à ceux-ci;

7.18.5. Examiner, concevoir et élaborer des documents techniques liés au SIEM, entre autres : des lignes directrices administratives, des lignes directrices liées aux services de soutien, des procédures opérationnelles normalisées, des plans de mise l'essai, etc.;

7.18.6. Exécuter la surveillance de la sécurité des réseaux et faire une analyse des journaux afin de détecter les activités malveillantes;

7.18.7. Déployer et exploiter tous les aspects d'une solution SIEM;

7.18.8. Participer aux réunions et aux groupes de travail hebdomadaires ou mensuels à la demande du RT;

7.18.9. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;

7.18.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT) en appui au programme ministériel de cyberprotection et de sécurité des TI.

8. EXIGENCES EN MATIÈRE DE RAPPORTS

8.1. L'entrepreneur doit présenter un rapport de progression mensuel pour chacune des ressources et l'envoyer au RT au début du mois suivant. Une copie de ce rapport doit également être jointe à la facture mensuelle. Chacun de ces rapports doit contenir au moins les renseignements suivants :

8.1.1. Toutes les activités importantes réalisées au cours de la période visée susceptibles d'avoir une incidence sur le rendement des travaux;

8.1.2. L'état de toute activité non terminée qui peut dépasser les délais normaux;

8.1.3. La description des problèmes rencontrés qui nécessiteront une attention ou qui pourraient s'aggraver;

8.1.4. Des recommandations visant à mettre à jour les procédures.

8.2. Tous les rapports doivent être remis dans un format acceptable aux yeux du RT.

ANNEXE A – ÉNONCÉ DES TRAVAUX
VOLET DE TRAVAIL 2 – TRÈS SECRET

9. EXIGENCES LINGUISTIQUES

9.1. Chacune des autorisations de tâches précisera les exigences linguistiques.

9.1.1. Les ressources doivent maîtriser l'anglais pour toutes les tâches. Par « maîtriser », on entend la capacité à communiquer de vive voix ou par écrit, sans aide et en faisant peu d'erreurs.

10. LIEU DE TRAVAIL

10.1. Tous les travaux doivent être accomplis dans les installations du MDN au sein de la RCN.

11. DÉPLACEMENTS

11.1. Les frais de déplacement au sein de la RCN ne seront pas remboursés.

11.2. Si, pendant la période du contrat, des déplacements s'avèrent nécessaires à l'extérieur de la RCN, les factures de frais de déplacement et de subsistance présentées doivent être accompagnées de pièces justificatives (reçus) et seront remboursées conformément à la politique et aux lignes directrices du Conseil du Trésor sur les voyages en vigueur au moment des déplacements, au coût réel, sans provision pour la marge bénéficiaire ou le profit. Tous les déplacements à l'extérieur de la RCN doivent être approuvés au préalable par le RT par écrit.

APPENDICE C DE L'ANNEXE A
CRITÈRES D'ÉVALUATION DES RESSOURCES ET TABLEAU DE RÉPONSE
VOLET DE TRAVAIL 1 – SECRET

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 soumissionnaires 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 devrait être fournie.

CRITÈRES LIÉS AUX RESSOURCES

CRITÈRES OBLIGATOIRES

C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2
Titre de tâche spécifique : Security Technical Implementation Guide (Guide de mise en œuvre technique de la sécurité)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2 Titre de tâche spécifique : Security Technical Implementation Guide (Guide de mise en œuvre technique de la sécurité)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la rédaction de documents sur les politiques et/ou d'exigences en matière de sécurité.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la rédaction de documents de configuration technique et/ou de mise en œuvre technique.			
	Conforme (oui/non)?			

C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3
Titre de tâche spécifique : ICP

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3 Titre de tâche spécifique : ICP				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée, acquise au cours des quinze (15) dernières années, de la conception et de la prestation de solutions d'ICP.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la préparation de documents sur l'ingénierie des systèmes (p. ex., analyse des options, conception, élaboration, mise à l'essai et mise en œuvre).			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée, acquise au cours des cinq (5) dernières années, de l'intégration de solutions d'ICP à des services d'entreprise, dont les services suivants : • Active Directory; • service d'annuaire X.500; • protection contre les codes malveillants et protection au niveau des systèmes hôtes; • services de pare-feu.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
	Conforme (oui/non)?			

C.6 Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'ingénieur en sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problème de pare-feux.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipements de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de l'ingénierie d'environnements sécuritaires en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'intégration de validations de principe relatives à des solutions de sécurité de la TI.			
O6	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité des systèmes hôtes

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau2 Titre de tâche spécifique : Sécurité des systèmes hôtes				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des sept (7) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de capacités de protection de la sécurité des points d'extrémité au sein d'un environnement de TI d'entreprise. L'expérience en matière de capacités de protection de la sécurité des points d'extrémité doit comprendre deux (2) des éléments suivants : antivirus, prévention de la perte de données, balisage de données, gestion de droits relatifs aux données d'entreprise, détection des menaces relatives aux points d'extrémité et réponse connexe, pare-feu des systèmes hôtes, analyse et rétro-ingénierie des logiciels malveillants, contrôle des applications, prévention d'intrusion des systèmes hôtes, balisage et protection des données, analyse du comportement des utilisateurs et des entités, chiffrement de disques complets, chiffrement de supports amovibles.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de sécurité de la TI et des points d'extrémité au sein d'un environnement de TI d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai, de la tenue à jour et de la résolution de problèmes de l'équipement de sécurité de réseau suivant: • sentinelles et passerelles; • pare-feu; • service de protection des limites de réseau; • diodes de données; • mandataires Web • agent de transfert de courrier La ressource proposée doit posséder au moins deux (2) années d'expérience relativement à chacune des technologies susmentionnées.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai, de la tenue à jour et de la résolution de problèmes des produits et infrastructures de TI suivants: • système d'exploitation en réseau Microsoft; • réseaux IP; • intégration d'applications; • virtualisation. La ressource proposée doit posséder au moins trois (3) années d'expérience relativement à chacune des technologies susmentionnées.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L’entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d’expérience, acquise au cours des six (6) dernières années, de l’utilisation de réseaux communs classifiés au niveau Secret ou Très secret.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipement de réseau.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problèmes de pare-feu.			
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'intégration de validations de principe relatives à des solutions de sécurité de la TI.			
O6	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de la virtualisation

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de la virtualisation				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins huit (8) années d'expérience de l'utilisation de technologies de virtualisation.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquises au cours des quinze (15) dernières années dans les fonctions de spécialiste en conception de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience, acquise au cours des huit (8) dernières années, de la conception architecturale, de l'élaboration, de la mise à l'essai, de la mise en œuvre architecturales et du soutien en service relativement au logiciel Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15 000 utilisateurs.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquises au cours des dix (10) dernières années dans les fonctions d'analyste de la sécurité des réseaux.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel de sécurité Symantec Endpoint Protection au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel McAfee ePolicy Orchestrator au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de pare-feu.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de mandataires Web.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de transfert de courrier (MTA).			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de réseaux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des dix (10) dernières années, de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comportant au moins 500 utilisateurs.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la surveillance, de la configuration et de la mise au point d'outils de gestion de l'information et des événements de sécurité (SIEM) ou d'outils de saisie intégrale de paquets au sein d'un environnement de production.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2
Titre de tâche spécifique : Security Technical Implémentation Guide (Guide de mise en œuvre technique de la sécurité)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.2 – Analyste Des Méthodes, Politiques Et Procédures De Sécurité De La Ti – Niveau 2 Titre de tâche spécifique : Security Technical Implémentation Guide (Guide de mise en œuvre technique de la sécurité)					
C1	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la réalisation de conceptions d'architecture de sécurité.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation au sujet du renforcement de la sécurité d'hyperviseurs et de systèmes d'exploitation (p. ex., VMware vSphere, Microsoft Hyper-V, Microsoft Windows, Unix/Linux).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientations au sujet du renforcement de la sécurité d'applications clientes ou d'applications de serveur (p. ex., navigateurs Web, visionneuses ou éditeurs de documents, serveurs de base de données, serveurs de courriels, serveurs Web).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C4	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation au sujet du renforcement de la sécurité de dispositifs de réseautage (p. ex., routeurs, commutateurs, équilibreurs de charge, mandataires).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la mise en œuvre d'essais automatisés et de la validation automatisée de la configuration.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration ou la mise en œuvre de configurations de sécurité techniques de base.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C7	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation, ou de mise en oeuvre de tests de configuration respectant le protocole Security Content Automation Protocol (SCAP).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource détient au moins l'une des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Professional (SSCP); 3) GIAC Security Essentials Certification (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (https://www.cicdi.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 22 points**	**Note maximale : 31 points**		

C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3
Titre de tâche spécifique : ICP

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3 Titre de tâche spécifique : ICP					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des sept (7) dernières années, du soutien d'ICP à l'aide de l'une ou de plusieurs des technologies suivantes dans le cadre d'un projet de gestion de l'information et de technologie de l'information (GI-TI) : 1) Pare-feu; 2) Système de messagerie électronique; 3) Serveur Web; 4) Active Directory.	1 point = expérience minimale démontrée du soutien d'ICP à l'aide de l'une des technologies énumérées dans le cadre d'un projet de GI-TI. 2 points = expérience minimale démontrée du soutien d'ICP à l'aide de deux des technologies énumérées dans le cadre d'un projet de GI-TI. 3 points = expérience minimale démontrée du soutien d'ICP à l'aide de trois des technologies énumérées dans le cadre d'un projet de GI-TI. 4 points = expérience minimale démontrée du soutien d'ICP à l'aide des quatre technologies énumérées dans le cadre d'un projet de GI-TI.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	L'entrepreneur devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des sept (7) dernières années dans l'intégration de la technologie de cartes à puce relativement à des ICP.	2 points = expérience minimale démontrée en intégrant une (1) technologie de cartes à puce relativement à des ICP. 3 points = expérience minimale démontrée en intégrant deux (2) technologies de cartes à puce ou plus relativement à des ICP.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'intégration d'ICP avec des solutions de réseau privé virtuel (accès à distance protégé).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception et du déploiement de Microsoft Certificate Authority 2012 ou d'une version plus récente.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'intégration d'ICP avec une solution de gestion de l'identité (comme Oracle ou Tivoli).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration et de la mise en œuvre d'un plan de reprise après sinistre relatif aux ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration de politiques des certificats (Certificate Policies) et d'énoncés de pratiques relatives aux certificats (Certificate Practice Statement).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C8	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration de programmes de vérification relatifs au déploiement d'ICP et de la vérification du déploiement d'ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 25 points**		

C.6 Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'intégration, de la configuration et de la prestation de technologies Cisco, y compris de routeurs ou de commutateurs des séries Nexus et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la résolution de problèmes de pare-feu Palo Alto VM series.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de VMWare.	1 point : de 2 à 4 années d'expérience. 2 points : de 4 à 6 années d'expérience. 3 points : plus de 6 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de McAfee Web Gateway.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 année d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation des outils Web Application Firewall (WAF) et/ou Database Activity Monitoring (DAM) d'Imperva.	1 point : de 6 mois à 1 année d'expérience combinée. 2 points : plus de 1 à 2 années d'expérience combinée. 3 points : plus de 2 années d'expérience combinée.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de mandataires (proxies) réseau.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de générateurs de trafic orientés applications.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Professional (SSCP); 3) GIAC Security Essentials Certification (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (https://www.cicdi.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité des systèmes hôtes

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité des systèmes hôtes					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'application de politiques gouvernementales de sécurité de la TI visant la protection des points d'extrémité au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de capacités de sécurité Microsoft au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de politiques de sécurité McAfee pour des points d'extrémité au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'ingénierie, de l'intégration ou du soutien des outils de gestion McAfee, Symantec ou Trend-Micro pour l'optimisation d'environnements virtuels au sein d'un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'évaluation de diverses technologies de sécurité et de la documentation d'analyses aux fins de prise de décision par les dirigeants.	1 point par projet jusqu'à un maximum de 3 projets*† *Si un soumissionnaire fournit plus de 3 projets en réponse à ce critère, seuls les 3 premiers projets cités seront évalués. †Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède d'expérience combinée de l'ingénierie et de la mise en œuvre de solutions de sécurité réseau à l'aide d'au moins trois (3) des technologies de sécurité réseau suivantes : 1) Système de détection d'intrusion et système de prévention d'intrusion; 2) Pare-feu/solutions UTM; 3) Saisie intégrale des paquets; 4) Mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et points d'accès (TAP); 7) Surveillance des activités de base de données; 8) Contrôle de l'accès réseau (802.1x); 9) Autres systèmes d'inspection de contenu. Un minimum de trois mois d'expérience est requis dans chaque domaine identifié pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) Certification ISC2 Certified Information System Security Professional (CISSP); 2) Certification ISC2 Certified Cloud Security Professional (CCSP); 3) Certification ISC2 Systems Security Certified Professional (SSCP); et/ou 4) Certification Global Information Assurance Certification (GIAC). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de mandataires comme McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier Trustwave MailMarshall Secure Email Gateway.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la prestation de technologies Cisco, y compris de routeurs et/ou de commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'intégration, de la configuration et de la prestation de technologies Cisco, y compris de routeurs et/ou de commutateurs des séries Nexus et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la résolution de problèmes de pare-feu Palo Alto VM-series.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de générateurs de trafic orientés applications.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de systèmes de détection d'intrusion (IDS).	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 2 à 4 années d'expérience. 2 points : plus de 4 à 6 années d'expérience. 3 points : plus de 6 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la prestation d'équilibreurs de charge F5.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de technologies de chiffrement réseau en série.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 22 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de la virtualisation

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de la virtualisation					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie Hyper-V.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation d'un centre de données virtuel.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception de solutions d'infrastructure de postes de travail virtuelle.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la prestation de conseils en matière de sécurité relativement aux infrastructures virtuelles.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'intégration de contrôles de sécurité de tiers au sein d'infrastructures virtuelles.	2 points = 1 projet. 3 points = 2 projets. 4 points = 3 projets ou plus. Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	4		
C8	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la préparation de plans de continuité des activités et de plans de reprise après sinistre ou de la réalisation d'analyses connexes.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
	Total :	**Note de passage minimale : 22 points**	**Note maximale : 32 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception architecturale relativement à la solution Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	3 points : plus de 4 à 5 années d'expérience. 4 points : plus de 5 à 6 années d'expérience. 5 points : plus de 6 années d'expérience.	5		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception architecturale relativement à la solution de sécurité Symantec Endpoint Protection au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'application de politiques gouvernementales de sécurité de la TI visant la protection des points d'extrémité au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède d'expérience combinée de l'analyse des éléments suivants : 1) outils et techniques de sécurité de la TI; 2) données de sécurité, présentation d'avis et de rapports concernant celles-ci; 3) statistiques sur la sécurité de la TI.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède d'expérience combinée de la rédaction de rapports techniques, tels que des analyses des exigences, des analyses des options et des documents d'architecture technique.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de politiques relatives aux pare-feu au niveau de l'hôte gérés de façon centralisée.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède plus d'une (1) année d'expérience de la prestation d'un soutien technique pour au moins une des technologies de sécurité au niveau de l'hôte suivantes au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs : 1) Stormshield Endpoint Security; 2) Symantec Endpoint Protection; et 3) McAfee ePolicy Orchestrator.	3 points : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 4 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 5 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	5		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre et du codage des règles F5 Big-IP iRules.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de règles relatives à un système de détection des intrusions au niveau de l'hôte géré de façon centralisée.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinées de la configuration et du soutien des systèmes d'exploitation suivants: 1) Windows 7; 2) Windows Server 2008; et/ou 3) Windows Server 2012.	2 points : d'expérience combinée minimale démontrée pour un (1) des systèmes d'exploitation figurant dans la liste. 3 points : d'expérience combinée minimale démontrée pour deux (2) des systèmes d'exploitation figurant dans la liste. 4 points : d'expérience combinée minimale démontrée pour les trois (3) systèmes d'exploitation figurant dans la liste.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la prestation du soutien de serveurs Syslog.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la tenue à jour de bases de données MS SQL (Microsoft Structured Query Language).	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
	Total :	**Note de passage minimale : 20 points**	**Note maximale : 29 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de mandataires comme McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier Trustwave MailMarshall Secure Email Gateway.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la conception et de la configuration de la distribution du trafic des applications à l'aide de produits F5 (technologies DNS, LTM et BIGIP).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologie de réseaux Cisco, y compris de protocoles de routage dynamique (p. ex., BGP, OSPF), la séparation de réseaux (p. ex., VRF, VLAN) et la traduction d'adresse réseau (NAT).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C8	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des dix (10) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : plus de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, en configuration, amélioration et optimisation d'un système de gestion des informations et des événements de sécurité (GIES) dans un environnement de production ou de solutions de saisie intégrale des paquets (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise dans un environnement de 500 à 5 000 utilisateurs. 2 points = expérience acquise dans un environnement de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise dans un environnement de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la prestation de services de détection, d'analyse et de gestion des incidents liés à la sécurité de la TI au moyen d'outils automatisés de GIES.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation et de la configuration de tous les aspects : 1) d'une solution de GIES, y compris la normalisation des données, la transmission des fichiers journaux, le regroupement d'éléments journaux, le stockage des événements et journeaux, l'établissement d'une corrélation entre les fichiers journaux et les événements et la production de rapports et d'alertes; ou 2) d'une solution de saisie intégrale des paquets, y compris la surveillance, la saisie, la collecte, la production et l'analyse de métadonnées.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée a suivi une formation spécifique relative à ArcSight ou à RSA Netwitness ou qu'elle détient une certification relative à la technologie ArcSight ou à la technologie RSA Netwitness.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de l'examen, de l'élaboration et de la mise en œuvre de flux de processus de traitement et d'escalade des incidents dans le cadre d'un projet de GI-TI.	1 point = 1 projet. 2 points = 2 projets. 3 points = 3 projets ou plus. Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource détient au moins l'une des certifications suivantes : 1) International Information System Security Certification Consortium (ISC)^2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA); 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 14 points**	**Note maximale : 20 points**		

APPENDICE C DE L'ANNEXE A

CRITÈRES D'ÉVALUATION DES RESSOURCES ET TABLEAU DE RÉPONSE

VOLET DE TRAVAIL 2 – TRÈS SECRET

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 soumissionnaires 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 devrait être fournie.

CRITÈRES LIÉS AUX RESSOURCES

CRITÈRES OBLIGATOIRES

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de la configuration

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de la configuration				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la planification et de la mise en œuvre de solutions de sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de l'exécution des tâches liées à la conception de l'architecture de sécurité ou au soutien en ingénierie dans le domaine de la sécurité de la TI.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, au cours des dix (10) dernières années, de la planification, de l'élaboration, de la mise en œuvre et de l'intégration de solutions d'évaluation de la vulnérabilité.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de l'élaboration et de la mise en œuvre d'un programme de gestion des vulnérabilités pour une organisation comptant au moins 5 000 utilisateurs.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'application des politiques de sécurité de la TI du gouvernement.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées à un serveur mandataire Web.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration de solutions de service de protection des limites de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Architecture de référence pour la cybersécurité

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Architecture de référence pour la cybersécurité				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de la planification et/ou de la mise en œuvre des services de technologie de l'information, tels que les services Web, les services de bases de données, les services d'annuaire, les services d'accès utilisateurs, les environnements virtuels et/ou les postes de travail virtuels.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'examen, de la conception, de la planification et/ou de la mise en œuvre de services de sécurité ou de l'architecture de sécurité des systèmes de TI soutenant plus d'une centaine d'utilisateurs.			
O3	L'entrepreneur doit démontrer que la ressource proposée a acquis au moins cinq (5) années d'expérience de la rédaction de documents techniques de configuration ou de mise en œuvre.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de l'élaboration, de la configuration et de la mise à l'essai de contrôles et de politiques de sécurité de réseau.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception et de la prestation de services de postes de travail virtuels.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception, de la configuration et de la mise en œuvre de modèles de contrôle d'accès fondés sur les rôles et sur des règles.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • les spécifications de la conception du système; • les documents sur la construction et la configuration; • le concept d'opérations (ConOp); • les plans de mise en œuvre de systèmes; • les plans d'essais et les rapports de mises à l'essai; et • les plans de soutien du cycle de vie.			
O6	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception, de la configuration et de la mise en œuvre de modèles de canal sécurisé IPSec.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Solution interdomaine – Transfert

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Solution interdomaine – Transfert				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies 'High Assurance Guard'.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration des technologies de filtre de contenu de courriel (comme la protection contre les logiciels malveillants) et de prévention de la perte de données (par exemple, le contrôle de label et la vérification du vocabulaire).			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • les spécifications de la conception du système; • les documents sur la construction et la configuration; • le concept d'opérations (CONOP); • les plans de mise en œuvre de systèmes; • les plans d'essais et les rapports de mises à l'essai; • les plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux serveurs mandataires Web.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration de solutions de service de protection des limites de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'ingénieur en sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée de la rédaction et de la tenue à jour de la documentation technique et d'ingénierie sur la gestion des informations et des événements de sécurité (SIEM) et la saisie intégrale des paquets (Full Packet Capture).			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la surveillance de la sécurité des réseaux dans un environnement de déploiement d'entreprise.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la conception, du déploiement et de l'intégration des outils de GIES (SIEM) ou de la saisie intégrale des paquets dans un environnement de production.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Saisie intégrale des paquets

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Saisie intégrale des paquets				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de la conception, du déploiement, de l'administration ainsi que de la résolution de problèmes de composants de l'infrastructure de communication du réseau local ou étendu.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de l'administration du système Linux ou d'une variante de Linux.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité de l'hôte

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité de l'hôte				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des sept (7) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de capacités de sécurité visant à protéger les points d'extrémité dans un environnement de TI d'entreprise. L'expérience relative logiciels de sécurité pour la protection des points d'extrémité doit comprendre deux (2) des éléments suivants : antivirus, prévention de la perte de données (PPD), balisage de données, la gestion des droits liés aux données d'entreprise, logiciel Endpoint detection and response (EDR), pare−feu hôte, analyse et ingénierie inverse des logiciels malveillants, contrôle des applications, prévention des intrusions au niveau de l'hôte, balisage et protection des données, analytique des comportements des utilisateurs et des entités (UEBA), chiffrement intégral de disque et chiffrement de supports amovibles.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de protection des points d'extrémité de sécurité de la TI dans un environnement de TI d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'élaboration d'une conception d'architecture de sécurité pour une solution classifiée du gouvernement (dont la classification est « Secret » ou supérieure).			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'utilisation d'au moins un (1) des procédés ou cadres architecturaux suivants : • TOGAF (The Open Group Architecture Framework); • FEAP (gouvernement américain); • Programme de transformation opérationnelle du gouvernement du Canada; • Zachman; ou • Cadre d'architecture de sécurité SABSA (Sherwood Applied Business Security Architecture Institute)			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'analyse d'exigences, de la conception et de la mise en œuvre des exigences relatives à la solution de GIJIA.			
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de la prestation de séances d'information à l'intention des cadres supérieurs (niveaux des directeurs et niveaux supérieurs) relatives aux considérations en matière de sécurité de la TI et aux mesures recommandées.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai et de la tenue à jour de l'équipement des technologies sécurité de réseau suivant et de la résolution de problèmes connexes : • sentinelles et passerelles; • pare-feu; • service de protection des limites de réseau; • diodes de données; • serveurs mandataires Web; • agent de transfert de courrier. La ressource proposée doit posséder au moins deux (2) années d'expérience relativement à chacune des technologies susmentionnées.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai et de la tenue à jour des produits et infrastructures de TI suivants et de la résolution de problèmes connexes : • système d'exploitation en réseau Microsoft; • réseaux IP; • intégration d'applications; • virtualisation. La ressource proposée doit posséder au moins trois (3) années d'expérience relativement à chacune des technologies susmentionnées.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; et • plans de soutien du cycle de vie.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des six (6) dernières années, de l'utilisation de réseaux classifiés communs au niveau « Secret » ou « Très secret ».			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la planification et de la mise en œuvre d'architectures d'intégration de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception et de la mise en œuvre de contrôles et de politiques de sécurité de réseau ainsi que de la gestion du changement à cet égard.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de services de postes de travail virtuels ainsi que de la gestion du changement à cet égard.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de modèles de contrôle d'accès fondés sur les rôles et sur des règles ainsi que de la gestion du changement à cet égard.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de modèles de canal sécurité IPSec ainsi que de la gestion du changement à cet égard.			
O6	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de l'hôte

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de l'hôte				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la conception et de la mise en œuvre de solutions de sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de logiciels de sécurité visant à protéger les points d'extrémité dans un environnement de TI d'entreprise. L'expérience relative logiciels de sécurité pour la protection des points d'extrémité doit comprendre trois (3) des éléments suivants : antivirus, prévention de la perte de données (PPD), balisage de données, gestion des droits liés aux données d'entreprise, logiciel Endpoint detection and response (EDR), pare-feu hôte, analyse et ingénierie inverse des logiciels malveillants, contrôle des applications, prévention des intrusions au niveau de l'hôte, balisage et protection des données, analytique des comportements des utilisateurs et des entités (UEBA), chiffrement intégral de disque et chiffrement de supports amovibles.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de l'application des politiques de protection des points d'extrémité de sécurité de la TI dans un environnement de TI d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée dans l'élaboration d'au moins trois (3) différents types de documents sur l'ingénierie des systèmes suivants: • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipement de réseau.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des dix (10) dernières années, de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problèmes de pare-feux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L’entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d’expérience de l’intégration de validations de principe relatives à des solutions de sécurité de la TI.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de l'élaboration et de la mise en œuvre d'une solution axée sur la gouvernance d'entreprise, la gestion des risques et la conformité pour une organisation comptant au moins 5 000 utilisateurs.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de l'évaluation des contrôles de sécurité, de l'évaluation de la menace et des risques associés à un système de TI ou de l'interprétation et de l'application des lignes directrices énoncées à l'annexe A des *Conseils en matière de sécurité des technologies de l'information (ITSG) 33*.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des dix (10) dernières années, de la définition des exigences, de la transformation des processus opérationnels en un flux des travaux et de l'ingénierie de solutions aux stades de la définition et de la mise en œuvre d'un projet de sécurité de la TI.			
	Conforme (oui/non)?			

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comptant au moins 500 utilisateurs.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la collecte et de l'analyse de codes malveillants des hôtes et du trafic sur le réseau.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la surveillance, de la configuration et de la mise au point d'outils GIES ou de la saisie intégrale des paquets dans un environnement de production.			
	Conforme (oui/non)?			

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de la configuration et de la prestation d'un soutien technique pour l'outil de gestion des informations et des événements de sécurité (GIES) ArcSight dans un environnement de production.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comptant au moins 500 utilisateurs.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la GIES pour les serveurs et les postes de travail dans un environnement de déploiement d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L’entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d’expérience de la conception, de la configuration et de la résolution de problèmes de serveurs Linux.			
	Conforme (oui/non)?			

C.12 – Spécialiste de la gestion des incidents – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.12 – Spécialiste de la gestion des incidents de niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)				
O1	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste de la gestion des incidents.			
O2	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de la mise en œuvre et de la prestation de soutien technique pour l'outil de gestion des informations et des événements de sécurité (GIES) ArcSight dans un environnement de production.			
O3	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la GIES pour les serveurs et les postes de travail dans un environnement de déploiement d'entreprise.			
O4	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception, de la configuration et de la résolution de problèmes de serveurs Linux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	L’entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d’expérience de la création et de la tenue à jour de documents ou de produits livrables d’ingénierie sur la GIES.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de la configuration

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de la configuration					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'application des politiques du gouvernement en matière de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'analyse des options relatives aux outils et aux techniques de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la planification, de l'élaboration, de la mise en œuvre et de l'intégration des solutions de détection de biens de TI et de base de données de gestion de la configuration (BDGC).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la planification, de l'élaboration, de la mise en œuvre et de l'intégration de solutions automatisées de vérification de la conformité des configurations.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la rédaction de rapports techniques comme les documents d'analyse des exigences, d'analyse des options et d'architecture technique.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'élaboration de guides de renforcement de la sécurité des systèmes de TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1. Certified Information System Security Professional (CISSP); 2. Systems Security Certified Practitioner (SSCP); 3. GIAC Security Essentials (GSEC); 4. Microsoft Certified Solutions Expert (MCSE); 5. Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 19 points**	**Note maximale : 27 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de serveurs mandataires, comme le McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier pour la passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Architecture de référence pour la cybersécurité

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Architecture de référence pour la cybersécurité					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de la conception, de façon individuelle ou conjointe, d'un environnement de TI à grande échelle pour au moins 100 utilisateurs.	Soutien pour les utilisateurs de la TI 3 points : de 100 à 300 utilisateurs. 4 points : de 300 à 1 000 utilisateurs. 5 points : 1 000 utilisateurs et plus.	5		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la mise en application des processus de gestion des risques pour la sécurité de la TI ou des processus d'ingénierie pour la sécurité des systèmes.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de méthodes de détection d'intrusion de la TI et de protection contre l'intrusion de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de solutions de surveillance de système axée sur les accès, les changements ou l'état de fonctionnement.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de services de TI d'entreprise, notamment les services de répertoire, d'authentification unique, de courriel, de sauvegarde ou de base de données distribuée pour un système de TI utilisé par au moins 500 utilisateurs.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration des principes de défense en profondeur de la TI. L'entrepreneur doit démontrer la façon dont la ressource a mis en application ces principes et en fournir une description.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'utilisation d'un cadre d'architecture d'entreprise reconnu.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C8	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la rédaction de documents techniques destinés à un personnel organisationnel à l'aide des outils bureautiques.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 4 années d'expérience. 3 points : plus de 4 à 6 années d'expérience. 4 points : plus de 6 années d'expérience.	4		
	Total :	**Note de passage minimale : 19 points**	**Note maximale : 27 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Solution interdomaine – Transfert

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Solution interdomaine – Transfert					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de serveurs mandataires, comme le McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier pour la passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Red Hat Enterprise Linux (RHEL).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, de l'expérience dans l'ingénierie de solutions de surveillance de la sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité suivantes : a. sécurité au niveau de l'hôte; b. système de détection d'intrusion et système de prévention d'intrusion (IDS/IPS); c. pare-feu et produits de gestion unifiée des menaces (UTM); d. saisie intégrale des paquets e. serveurs mandataires; f. équilibreurs de charge; 7) commutateurs matriciels et prises réseau (Taps).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	L'entrepreneur devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou sur la plateforme RSA Netwitness ou qu'elle détient une certification à jour sur la technologie ArcSight ou la technologie RSA Netwitness. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, de l'expérience dans la conception de solutions de surveillance de la sécurité des réseaux pour le gouvernement s'appuyant sur les directives de sécurité des TI (DSTI) 02 ou les conseils en matière de sécurité des TI (ITSG) 22 au niveau « Protégé B » ou supérieur.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la prestation de services d'ingénierie de sécurité de la TI pour des ministères et des organismes du gouvernement sous forme de développement d'architecture de sécurité, de conseils et de directives connexes.	1 point : de 3 à 5 années d'expérience. 2 points : plus de 5 à 7 années d'expérience. 3 points : plus de 7 à 9 années d'expérience. 4 points : plus de 9 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1) International Information System Security Certification Consortium (ISC)^2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH) 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux http://www.cicic.ca/1/accueil.canada	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 16 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Saisie intégrale des paquets

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Saisie intégrale des paquets					
C1	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception, la planification et la mise en œuvre d'une infrastructure de réseau d'environnements complexes et hautement accessibles*. *On entend par « environnements complexes et hautement accessibles », des environnements qui touchent plusieurs villes ou pays et pour lesquels aucun temps d'interruption de service n'est permis.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

C2	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, d'expérience combinée dans la réalisation d'au moins une des activités de TI suivantes : 1. Rédaction de rapports techniques comme les documents d'analyse des exigences, d'analyse des options, d'artéfacts de processus d'ingénierie ou de l'architecture technique; 2. Automatisation de l'administration des systèmes Linux au moyen de scripts et d'interfaces de programmation d'applications comme les langages Ruby, PHP, Bash, Perl ou Python; 3. Analyse des données brutes relatives au trafic sur le réseau à l'appui de la résolution de problèmes ou de l'analyse judiciaire des réseaux; 4. Déploiement et administration de dispositifs de surveillance du trafic du réseau ou d'analyse judiciaire des réseaux comme FireEye, Solera, Sourcefire et Cisco, système de détection ou de prévention d'intrusion, SNORT ou Netwitness (RSA Security Analytics); 5. Examen des alertes et des paquets provenant de capteurs de détection d'intrusion (IDS) ou de dispositifs de saisie des paquets;	1 point : de 6 à 9 mois d'expérience. 2 points : plus 9 à 12 mois d'expérience. 3 points : plus 12 à 15 mois d'expérience. 4 points : plus 15 mois d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	6. Analyse de logiciels malveillants et analyse de type bac à sable à l'aide d'applications comme Netwitness Spectrum et RSA Malware, WireShark, CaptureBAT ou Cuckoo Sandbox et la capacité d'ingénierie inversée et de débogage des logiciels malveillants à l'aide d'outils comme IDA Pro, Responder Pro ou OllyDbg, y compris des techniques de défense contre l'antidébogage, l'élaboration de trousses et le brouillage. 7. Gestion des technologies de réseau de stockage (SAN) et NAS – canal de fibre optique, FCOE (canal de fibre optique sur réseau Ethernet), iSCSI (interface de système pour microordinateur sur Internet), serveur NFS (système de fichiers en réseau), protocole CIFS, notamment des numéros d'unité logique, le câblage, la résolution de problèmes et les correctifs. Un minimum de trois (3) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.				

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) RSA Security Analytics Certified Administrator; 2) Toute certification Cisco de niveau « Associé »; 3) Toute certification Cisco de niveau « Professionnel »; 4) Toute certification Cisco de niveau « Expert »; 5) Toute certification GIAC du SANS institute dans la catégorie « Security Administration »; 6) Toute certification Red Hat Certified System Administrator, Red Hat Certified Engineer ou Red Hat Certified Architect. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 certifications ou plus.	5		
	Total :	**Note de passage minimale : 8 points**	**Note maximale : 12 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité de l'hôte

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité de l'hôte					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède au moins un (1) an d'expérience de l'application de politiques de protection des points d'extrémité de sécurité de la TI du gouvernement dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte géré de façon centralisée dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte de McAfee, Symantec ou Trend-Micro dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'ingénierie et de la mise en œuvre de chacune des technologies de sécurité au niveau de l'hôte dans un environnement de TI d'entreprise suivantes : 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; 3) 3) Trend-Micro Control Manager.	1 point : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 2 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 3 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de l'intégration ou du soutien des logiciels de gestion de McAfee, Symantec ou Trend-Micro pour les environnements virtuels optimisés dans un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'évaluation de diverses technologies de sécurité de la TI et de la documentation d'une analyse aux fins de prise de décision de la direction.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie et de la mise en œuvre de solutions de sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité des réseaux suivantes : 1) système de détection d'intrusion et système de prévention d'intrusion (IDS/IPS); 2) pare-feu et produits de gestion unifiée des menaces (UTM); 3) Saisie intégrale des paquets; 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prise réseaux (Taps); 7) Surveillance de l'activité de la base de données; 8) Contrôle de l'accès au réseau (802.1x); 9) Autres systèmes d'inspection de contenu Un minimum de trois (3) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); 4) Toute certification Global Information Assurance Certification (GIAC). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 certifications ou plus.	5		
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 26 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)					
C1	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration de procédures opérationnelles normalisées (PON) pour des projets.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception et le déploiement de technologies liées aux ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception et le déploiement de solutions de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de la conception de solutions de TI qui nécessitent une interopérabilité avec les systèmes : • d'un ou plusieurs ministères du gouvernement du Canada; ou • d'un ou plusieurs des partenaires internationaux suivants : les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.	1 point : expérience d'au moins six (6) mois démontrée dans la conception de solutions de TI qui exigent une interopérabilité avec les systèmes des ministères du gouvernement du Canada. 2 points : expérience d'au moins six (6) mois démontrée dans la conception de solutions de TI qui exigent l'interopérabilité avec les systèmes de partenaires internationaux (États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande)	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception de schémas de processus pour un concept d'architecture de sécurité.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre des technologies de serveurs mandataires, comme la passerelle Web McAfee, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal) et d'agent de transfert de courrier.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine au sein de grands réseaux de TI (comptant au moins 1 000 utilisateurs).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'application des politiques de sécurité de la TI du gouvernement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	L'entrepreneur devrait démontrer que la ressource proposée possède d'expérience combinée de la réalisation des trois (3) tâches de sécurité des TI suivantes : 1) analyse des outils et des techniques de sécurité de la TI; 2) analyse des données de sécurité et présentation d'avis et de rapports; 3) rédaction de rapports techniques, y compris les documents d'analyse des exigences, d'analyse des options, d'architecture technique et de modélisation des risques mathématiques; 4) conception de l'architecture de sécurité et soutien d'ingénierie; 5) études liées à la classification de la sécurité des données. Un minimum de six (6) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la conception et de la mise en œuvre et de la gestion du changement liées aux technologies VMWare	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée détient au moins l'une des certifications suivantes dans le domaine de l'architecture : 1) Certification TOGAF (The Open Group Architecture Framework) 2) Certification en Gestion des services en technologie de l'information (GSTI) 3) Certification du EACOE (Enterprise Architecture Center of Excellence) 4) Certification Microsoft Certified Architect (MCA); 5) Certification VMware Certified Design Expert (VCDX). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de l'hôte

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de l'hôte					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de protection des points d'extrémité de la sécurité de la TI du gouvernement dans un environnement de TI d'entreprise.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte géré de façon centralisée dans un environnement de TI d'entreprise.	1 point : de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité sur un hôte McAfee dans un environnement de TI d'entreprise.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	L'entrepreneur devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'ingénierie et de la mise en œuvre pour chacune des technologies de sécurité au niveau de l'hôte dans un environnement de TI d'entreprise suivantes : 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; 3) 3) Trend-Micro Control Manager.	1 point : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 2 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 3 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de l'intégration ou du soutien des logiciels de gestion de McAfee, Symantec ou Trend-Micro pour les environnements virtuels optimisés dans un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une l'expérience de l'évaluation de diverses technologies de sécurité de la TI et de la documentation d'une analyse aux fins de prise de décision de la direction.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'ingénierie et de la mise en œuvre de solutions de sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité des réseaux suivantes : 1) SDI/SPI 2) Pare-feu et produits UTM; 3) Saisie intégrale des paquets; 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseau (Taps); 7) Surveillance de l'activité de la base de données; 8) Contrôle de l'accès au réseau (802.1x); 9) Autres systèmes d'inspection de contenu Un minimum de six (6) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution de technologies Cisco, y compris les routeurs ou les commutateurs de série NEXUS et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration ainsi que de la résolution de problèmes de solutions de pare-feu Palo Alto.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'utilisation d'outils de génération de trafic en fonction de l'application.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'utilisation de systèmes de détection d'intrusion (IDS).	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'utilisation de VMWare.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution des équilibreurs de charge F5.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'utilisation des technologies de chiffrement de réseau en série.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP) 3) GIAC Security Essentials (GSEC) 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 25 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité					
C1	L'entrepreneur devrait démontrer que la ressource proposée détient au moins l'une des certifications suivantes dans le domaine de l'administration des applications axées sur la gouvernance, la gestion des risques et la gestion de la conformité de TI ou d'entreprise : 1) RSA Archer Certified Administrator; 2) IBM OpenPages Administrator ; 3) MetricStream GRC Certified Administrator . Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	L'entrepreneur devrait démontrer que la ressource proposée a acquis au cours des cinq (5) dernières années, d'expérience combinée dans la création de transformation de données XML ou de scripts de traduction.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience des projets de conception de sécurité de la TI dans un environnement de mise en œuvre d'un cadre de gouvernance, de gestion des risques et de conformité d'entreprise (eGRC).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'application des politiques du gouvernement en matière de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, d'expérience combinée dans l'accréditation d'un système de TI au moyen du processus d'évaluation de sécurité et autorisation (SA&A) ou du programme de certification et d'accréditation (C&A).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C7	L'entrepreneur devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration des architectures de sécurité de réseau (niveau II ou supérieur) s'appuyant sur les directives de sécurité de la TI (DSTI) ou sur les *Conseils en matière de sécurité des technologies de l'information* (ITSG).	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP) 3) GIAC Security Essentials (GSEC) 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 16 points**	**Note maximale : 23 points**		

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience, acquise au cours des dix (10) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, aux tâches portant sur la configuration, l'amélioration et l'optimisation de solutions de gestion des informations et des événements de sécurité (GIES) ou de solutions de saisie intégrale des paquets (à l'exclusion des environnements de laboratoire) dans un environnement de production pour une grande organisation.	1 point = expérience acquise; soutien de 500 à 5 000 utilisateurs. 2 points = expérience acquise; soutien de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise; soutien de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de la prestation de services de détection, d'analyse et de gestion des incidents liés à la sécurité de la TI au moyen d'outils automatisés de GIES.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'exécution et de la configuration de tous les volets d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre journaux et événements, et la production de rapports et d'alertes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou sur la plateforme RSA Netwitness ou qu'elle détient une certification à jour sur la technologie ArcSight ou la technologie RSA Netwitness. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de l'examen, de l'élaboration et de la mise en œuvre de flux de processus de traitement et d'escalade d'incidents dans le cadre d'un projet de gestion de l'information et de technologie de l'information.	1 point – 1 projet. 2 points – 2 projets. 3 points – 3 projets ou plus. Un minimum de six (6) mois d'expérience est requis pour chaque projet afin qu'il soit pris en compte.	3		

C7	L'entrepreneur devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1) International Information System Security Certification Consortium (ISC)^2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 14 points**	**Note maximale : 20 points**		

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la surveillance de la sécurité des réseaux et de l'analyse des journaux pour détecter les activités malveillantes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue de la réalisation d'un projet portant sur la configuration, l'amélioration et la tenue à jour de solutions de gestion des informations et des événements de sécurité (GIES) dans un environnement de production (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise; soutien de 500 à 5 000 utilisateurs. 2 points = expérience acquise; soutien de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise; soutien de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la prestation d'un soutien technique pour au moins trois (3) des technologies de sécurité de réseau suivantes : 1) Sécurité au niveau de l'hôte; 2) Système de détection d'intrusion et système de prévention d'intrusion (SDI/SPI); 3) Pare-feu et produits de gestion unifiée des menaces (UTM); 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseaux (Taps).	1 point : de 2 à 5 mois d'expérience. 2 points : plus de 5 mois d'expérience.	2		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience du déploiement et de l'exécution de tous les aspects d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre les journaux et les événements, et la production de rapports et d'alertes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'amélioration et de la configuration des composants de la GIES afin d'en accroître l'efficacité, la précision et le rendement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de travail, acquise au cours des sept (7) dernières années, dans un environnement de soutien des services internes et de centre d'assistance.	1 point : de 1 à 6 mois d'expérience. 2 points : plus de 6 mois d'expérience.	2		
C7	L'entrepreneur devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou qu'elle détient une certification à jour relative à la technologie ArcSight. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
	Total :	**Note de passage minimale : 13 points**	**Note maximale : 18 points**		

C.12 – Spécialiste de la gestion des incidents – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.12 – Spécialiste de la gestion des incidents – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)					
C1	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	L'entrepreneur devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, travaillant à la configuration, l'amélioration et la tenue à jour de solutions de gestion des informations et des événements de sécurité (GIES) dans un environnement de production (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise dans un environnement de 500 à 5 000 utilisateurs. 2 points = expérience acquise dans un environnement de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise dans un environnement de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la prestation d'un soutien technique pour au moins trois (3) des technologies de sécurité de réseau suivantes : 1) Sécurité au niveau de l'hôte; 2) Système de détection d'intrusion et système de prévention d'intrusion (SDI/SPI); 3) Pare-feu et produits de gestion unifiée des menaces (UTM); 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseau (Taps).	1 point : de 2 à 5 mois d'expérience. 2 points : plus de 5 mois d'expérience.	2		
C4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience du déploiement et de l'exécution de tous les aspects d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre les journaux et les événements, et la production de rapports et d'alertes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de l'amélioration et de la configuration des composants de la GIES afin d'en accroître l'efficacité, la précision et le rendement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience de travail, acquise au cours des sept (7) dernières années, dans un environnement de soutien des services internes et de centre d'assistance.	1 point : de 1 à 6 mois d'expérience. 2 points : plus de 6 mois d'expérience.	2		
C7	L'entrepreneur devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou qu'elle détient une certification à jour relative à la technologie ArcSight. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
	Total :	**Note de passage minimale : 13 points**	**Note maximale : 18 points**		

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-17-P5LL S1 - Amendment 2
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

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

4. Brief Description of Work / Brève description du travail

Professional services using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as-required basis.

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

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

Canada ☑	NATO / OTAN ☑	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☐ SM	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays : Canada and USA	Specify country(ies): / Préciser le(s) pays : Canada and USA	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☑	NATO SECRET / NATO SECRET ☑	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☑	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

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

Special comments:
Commentaires spéciaux : _____

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

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-17-P5LL S2 - Amendment 2
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine **DND**	2. Branch or Directorate / Direction générale ou Direction DGIMTSP / DIMEI
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Professional services using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as-required basis.

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

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

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

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

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

Special comments:
Commentaires spéciaux : _____

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

10. b) May unscreened personnel be used for portions of the work? ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? ☐ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S1

Part A - Multiple Release Restrictions: Security Guide

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Canadian Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X					
Not Releasable							
Restricted to: Canada and USA				X	X		
Permanent Residents Included*							

NATO Information

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries					
Restricted to: Canada and USA				X	
Permanent Residents Included*					

Foreign Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							
Restricted to :							
Permanent Residents Included*							

COMSEC Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S1

Part B - Multiple Levels of Personnel Screening: Security Classification Guide **To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.**			
Level of Personnel Clearance (e.g. Reliability Status, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
NATO SECRET	IT Security Methodology, Policy and Procedures Analyst (Level 2)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	PKI Specialist (Level 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	IT Security Engineer (Level 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	IT Security Design Specialist (Level 2 and 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	Network Security Analyst (Level 2 and 3)	Up to and including NATO Secret	Canadian or US citizen

Part C – Safeguards / Information Technology (IT) Media – 11d = yes
IT security requirements must be specified in a separate technical document and submitted with the SRCL

OTHER SECURITY INTRUCTIONS

Insert instructions

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S2

Part A - Multiple Release Restrictions: Security Guide

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Canadian Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X					
Not Releasable				X	X	X	X
Restricted to:							
Permanent Residents Included*							

NATO Information

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries					
Restricted to: Canada				X	
Permanent Residents Included*					

Foreign Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							
Restricted to :							
Permanent Residents Included*							

COMSEC Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S2

Part B - Multiple Levels of Personnel Screening: Security Classification Guide **To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.**			
Level of Personnel Clearance (e.g. Reliability Status, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
NATO Secret and Top Secret-SIGINT	IT Security Engineer (Level 2 and 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	IT Security Design Specialist (Level 2 and 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	Network Security Analyst (Level 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	Incident Management Specialist (Level 3)	Up to and including Top Secret-SIGINT	Canadian citizen

Part C – Safeguards / Information Technology (IT) Media – 11d = yes
IT security requirements must be specified in a separate technical document and submitted with the SRCL

<u>OTHER SECURITY INTRUCTIONS</u>

Insert instructions

PIÈCE JOINTE 4.1

CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 1 – SECRET

1. Les critères d'évaluation de la présente pièce jointe serviront à évaluer les soumissions dans le cadre de l'appel d'offres et à faciliter l'évaluation des ressources après l'attribution du contrat.

2. Le soumissionnaire doit fournir un curriculum vitæ admissible pour chaque catégorie de ressources demandée aux fins d'évaluation (le soumissionnaire ne doit pas proposer la même ressource plus d'une fois en réponse au présent appel d'offres).

3. Le soumissionnaire doit remplir une grille d'évaluation pour chacun des curriculum vitæ fournis comme décrit dans le tableau 1 ci-dessous. Pour chaque critère, il doit indiquer la partie du curriculum vitæ où la conformité avec les critères est décrite. À défaut de fournir un curriculum vitæ admissible pour chaque catégorie de ressources, la soumission sera jugée non conforme.

Tableau 1 : Les soumissionnaires doivent soumettre le nombre suivant de curriculum vitæ par catégorie de ressources en réponse à la présente évaluation. Le nombre réel de ressources nécessaires est énuméré au point 1.2 Sommaire de la partie 1 de l'appel d'offres.

Catégorie de ressources avec titre de tâche spécifique	Niveau	Nombre de curriculum vitæ
C.2 Analyste des méthodes, politiques et procédures de sécurité de la TI Titre de tâche spécifique : Security Technical Implementation Guide (Guide de mise en œuvre technique de la sécurité)	2	1
C.5 Spécialiste de l'infrastructure à clé publique (ICP) Titre de tâche spécifique : ICP	3	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité des systèmes hôtes	2	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Passerelle d'échange d'information	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité de réseaux – Inspection du contenu	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité de la virtualisation	3	1
C.7 Spécialiste en conception de la sécurité de la TI	3	1

Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)		
C.8 Analyste de la sécurité des réseaux Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)	2	1
C.8 Analyste de la sécurité des réseaux Titre de tâche spécifique : Passerelle d'échange d'information	2	1
C.8 Analyste de la sécurité des réseaux Titre de tâche spécifique : Surveillance de la sécurité des réseaux	3	1

1. EXIGENCES POUR L'ORGANISATION

1.1. Exigences obligatoires pour l'organisation

EXIGENCES OBLIGATOIRES – CRITÈRES POUR L'ORGANISATION			
Point	**Critères obligatoires pour l'organisation**	**RESPECTÉ (oui/non)**	**Numéro de page du document de soumission**
O1	Le soumissionnaire doit s'être fait octroyer au moins deux (2) contrats de service professionnel en informatique† par un client gouvernemental*. Chacun des contrats mentionnés : 1. doit avoir une valeur d'au moins 5 millions de dollars (5 M$), taxes applicables en sus; 2. doit avoir eu une durée d'au moins deux (2) années, doit avoir été octroyé au cours des huit (8) dernières années précédant la date de clôture du présent appel d'offres et n'inclut pas les années d'option qui n'ont pas été exercées; 3. doit montrer que le soumissionnaire a fourni au moins cinq (5) ressources simultanément pendant une période d'au moins douze (12) mois consécutifs. Chacun des contrats mentionnés doit également montrer que le soumissionnaire a fourni des services à une organisation dans un milieu : • doté d'au moins 100 postes de travail connectés à un réseau protégé ou secret; • utilisant des systèmes d'exploitation Windows pour poste de travail (Windows XP, Windows Vista, Windows 7 ou Windows 10); • faisant appel à une gestion centralisée de la distribution de logiciels et des correctifs. Le soumissionnaire doit fournir une (1) référence pour chaque contrat. Chaque preuve de références doit inclure le nom de l'organisation, le numéro d'identification unique du contrat, une brève description des services fournis, le nom, le titre, l'adresse électronique et le numéro de téléphone du cadre responsable de l'organisation, le nombre de ressources fournies, ainsi que la date d'attribution, la date de fin et la valeur (en dollars) de chaque contrat. Il incombe au soumissionnaire de s'assurer que tout renseignement est divulgué avec la permission des références fournies. Le soumissionnaire doit avoir été l'entrepreneur principal, et non un sous-traitant. Autrement dit, le soumissionnaire a passé un contrat directement avec le client. Si le contrat		

	du soumissionnaire prévoyait qu'il devait effectuer des travaux pour lesquels les services d'une autre entité avaient d'abord été retenus par contrat, le soumissionnaire ne serait pas considéré comme l'entrepreneur principal. Par exemple, Z (le client) attribue à Y un contrat de service. Y, à son tour, passe un contrat avec X pour fournir une partie ou la totalité de ces services à Z. Dans cet exemple, Y est l'entrepreneur principal et X est le sous-traitant. Le soumissionnaire doit se rappeler qu'un arrangement en matière d'approvisionnement (AMA) ou une offre à commandes ne constitue pas un contrat et que, par conséquent, toute référence à ce type de documents sera exclue du processus d'évaluation de l'expérience du soumissionnaire en matière d'exécution de contrats. Par exemple, si le soumissionnaire cite en référence son numéro d'AMA des Services professionnels en informatique centrés sur les tâches (SPICT), tel que EN578-055605/XXX/EL, en guise de preuve de l'expérience aux termes des critères d'évaluation, le Canada ne tiendra pas compte de cette expérience, car elle ne se rapporte pas à un contrat particulier. *Client gouvernemental s'entend d'un ministère ou d'un organisme fédéral, provincial ou municipal ou d'une société d'État. †Les « services professionnels en informatique » sont des services professionnels fournis par le soumissionnaire à l'appui d'un projet ou d'un marché en technologie ou en gestion de l'information.		

CRITÈRES LIÉS AUX RESSOURCES

CRITÈRES OBLIGATOIRES

C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2
Titre de tâche spécifique : Security Technical Implementation Guide (Guide de mise en œuvre technique de la sécurité)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2 Titre de tâche spécifique : Security Technical Implementation Guide (Guide de mise en œuvre technique de la sécurité)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la rédaction de documents sur les politiques et/ou d'exigences en matière de sécurité.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la rédaction de documents de configuration technique et/ou de mise en œuvre technique.			
	Conforme (oui/non)?			

C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3
Titre de tâche spécifique : ICP

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3 Titre de tâche spécifique : ICP				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée, acquise au cours des quinze (15) dernières années, de la conception et de la prestation de solutions d'ICP.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la préparation de documents sur l'ingénierie des systèmes (p. ex., analyse des options, conception, élaboration, mise à l'essai et mise en œuvre).			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée, acquise au cours des cinq (5) dernières années, de l'intégration de solutions d'ICP à des services d'entreprise, dont les services suivants : • Active Directory; • service d'annuaire X.500; • protection contre les codes malveillants et protection au niveau des systèmes hôtes; • services de pare-feu.			
	Conforme (oui/non)?			

C.6 Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'ingénieur en sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problème de pare-feux.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipements de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, acquise au cours des dix (10) dernières années, de l'ingénierie d'environnements sécuritaires en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'intégration de validations de principe relatives à des solutions de sécurité de la TI.			
O6	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité des systèmes hôtes

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau2 Titre de tâche spécifique : Sécurité des systèmes hôtes				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des sept (7) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de capacités de protection de la sécurité des points d'extrémité au sein d'un environnement de TI d'entreprise. L'expérience en matière de capacités de protection de la sécurité des points d'extrémité doit comprendre deux (2) des éléments suivants : antivirus, prévention de la perte de données, balisage de données, gestion de droits relatifs aux données d'entreprise, détection des menaces relatives aux points d'extrémité et réponse connexe, pare-feu des systèmes hôtes, analyse et rétro-ingénierie des logiciels malveillants, contrôle des applications, prévention d'intrusion des systèmes hôtes, balisage et protection des données, analyse du comportement des utilisateurs et des entités, chiffrement de disques complets, chiffrement de supports amovibles.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de sécurité de la TI et des points d'extrémité au sein d'un environnement de TI d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai, de la tenue à jour et de la résolution de problèmes de l'équipement de sécurité de réseau suivant: • sentinelles et passerelles; • pare-feu; • service de protection des limites de réseau; • diodes de données; • mandataires Web • agent de transfert de courrier La ressource proposée doit posséder au moins deux (2) années d'expérience relativement à chacune des technologies susmentionnées.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai, de la tenue à jour et de la résolution de problèmes des produits et infrastructures de TI suivants: • système d'exploitation en réseau Microsoft; • réseaux IP; • intégration d'applications; • virtualisation. La ressource proposée doit posséder au moins trois (3) années d'expérience relativement à chacune des technologies susmentionnées.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des six (6) dernières années, de l'utilisation de réseaux communs classifiés au niveau Secret ou Très secret.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipement de réseau.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problèmes de pare-feu.			
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'intégration de validations de principe relatives à des solutions de sécurité de la TI.			
O6	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de la virtualisation

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de la virtualisation				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins huit (8) années d'expérience de l'utilisation de technologies de virtualisation.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquises au cours des quinze (15) dernières années, dans les fonctions de spécialiste en conception de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience, acquise au cours des huit (8) dernières années, de la conception, d'architetecture, de l'élaboration, de la mise à l'essai et de la mise en œuvre architecturales et du soutien en service relativement au logiciel Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15 000 utilisateurs.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquises au cours des dix (10) dernières années, dans les fonctions d'analyste de la sécurité des réseaux.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel de sécurité Symantec Endpoint Protection au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel McAfee ePolicy Orchestrator au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des cinq (5) dernières années, de la tenue à jour du logiciel Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de pare-feu.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de mandataires Web.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de transfert de courrier (MTA).			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration de technologies de réseaux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENTDANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.8 Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des dix (10) dernières années, de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comportant au moins 500 utilisateurs.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la surveillance, de la configuration et de la mise au point d'outils de gestion de l'information et des événements de sécurité (SIEM) ou d'outils de saisie intégrale de paquets au sein d'un environnement de production.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

C.2 – Analyste des méthodes, politiques et procédures de sécurité de la TI – Niveau 2
Titre de tâche spécifique : Security Technical Implémentation Guide (Guide de mise en œuvre technique de la sécurité)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.2 – Analyste Des Méthodes, Politiques Et Procédures De Sécurité De La Ti – Niveau 2 Titre de tâche spécifique : Security Technical Implémentation Guide (Guide de mise en œuvre technique de la sécurité)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la réalisation de conceptions d'architecture de sécurité.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation au sujet du renforcement de la sécurité d'hyperviseurs et de systèmes d'exploitation (p. ex., VMware vSphere, Microsoft Hyper-V, Microsoft Windows, Unix/Linux).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientations au sujet du renforcement de la sécurité d'applications clientes ou d'applications de serveur (p. ex., navigateurs Web, visionneuses ou éditeurs de documents, serveurs de base de données, serveurs de courriels, serveurs Web).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C4	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation au sujet du renforcement de la sécurité de dispositifs de réseautage (p. ex., routeurs, commutateurs, équilibreurs de charge, mandataires).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la mise en œuvre d'essais automatisés et de la validation automatisée de la configuration.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration ou la mise en œuvre de configurations de sécurité techniques de base.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C7	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la prestation d'orientation, ou de mise en oeuvre de tests de configuration respectant le protocole Security Content Automation Protocol (SCAP).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource détient au moins l'une des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Professional (SSCP); 3) GIAC Security Essentials Certification (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (https://www.cicdi.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 22 points**	**Note maximale : 31 points**		

C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3
Titre de tâche spécifique : ICP

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.5 Spécialiste de l'infrastructure à clé publique (ICP) – Niveau 3 Titre de tâche spécifique : ICP					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des sept (7) dernières années, du soutien d'ICP à l'aide de l'une ou de plusieurs des technologies suivantes dans le cadre d'un projet de gestion de l'information et de technologie de l'information (GI-TI) : 1) Pare-feu; 2) Système de messagerie électronique; 3) Serveur Web; 4) Active Directory.	1 point = expérience minimale démontrée du soutien d'ICP à l'aide de l'une des technologies énumérées dans le cadre d'un projet de GI-TI. 2 points = expérience minimale démontrée du soutien d'ICP à l'aide de deux des technologies énumérées dans le cadre d'un projet de GI-TI. 3 points = expérience minimale démontrée du soutien d'ICP à l'aide de trois des technologies énumérées dans le cadre d'un projet de GI-TI. 4 points = expérience minimale démontrée du soutien d'ICP à l'aide des quatre technologies énumérées dans le cadre d'un projet de GI-TI.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience, acquise au cours des sept (7) dernières années dans l'intégration de la technologie de cartes à puce relativement à des ICP.	2 points = expérience minimale démontrée en intégrant une (1) technologie de cartes à puce relativement à des ICP. 3 points = expérience minimale démontrée en intégrant deux (2) technologies de cartes à puce ou plus relativement à des ICP.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'intégration d'ICP avec des solutions de réseau privé virtuel (accès à distance protégé).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception et du déploiement de Microsoft Certificate Authority 2012 ou d'une version plus récente.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'intégration d'ICP avec une solution de gestion de l'identité (comme Oracle ou Tivoli).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration et de la mise en œuvre d'un plan de reprise après sinistre relatif aux ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration de politiques des certificats (Certificate Policies) et d'énoncés de pratiques relatives aux certificats (Certificate Practice Statement).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des sept (7) dernières années, de l'élaboration de programmes de vérification relatifs au déploiement d'ICP et de la vérification du déploiement d'ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 25 points**		

C.6 Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'intégration, de la configuration et de la prestation de technologies Cisco, y compris de routeurs ou de commutateurs des séries Nexus et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la résolution de problèmes de pare-feu Palo Alto VM series.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de VMWare.	1 point : de 2 à 4 années d'expérience. 2 points : de 4 à 6 années d'expérience. 3 points : plus de 6 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de McAfee Web Gateway.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 année d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation des outils Web Application Firewall (WAF) et/ou Database Activity Monitoring (DAM) d'Imperva.	1 point : de 6 mois à 1 année d'expérience combinée. 2 points : plus de 1 à 2 années d'expérience combinée. 3 points : plus de 2 années d'expérience combinée.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de mandataires (proxies) réseau.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de générateurs de trafic orientés applications.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Professional (SSCP); 3) GIAC Security Essentials Certification (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (https://www.cicdi.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité des systèmes hôtes

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité des systèmes hôtes					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'application de politiques gouvernementales de sécurité de la TI visant la protection des points d'extrémité au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de capacités de sécurité Microsoft au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de politiques de sécurité McAfee pour des points d'extrémité au sein d'un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'ingénierie, de l'intégration ou du soutien des outils de gestion McAfee, Symantec ou Trend-Micro pour l'optimisation d'environnements virtuels au sein d'un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'évaluation de diverses technologies de sécurité et de la documentation d'analyses aux fins de prise de décision par les dirigeants.	1 point par projet jusqu'à un maximum de 3 projets*† *Si un soumissionnaire fournit plus de 3 projets en réponse à ce critère, seuls les 3 premiers projets cités seront évalués. †Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède d'expérience combinée de l'ingénierie et de la mise en œuvre de solutions de sécurité réseau à l'aide d'au moins trois (3) des technologies de sécurité réseau suivantes : 1) Système de détection d'intrusion et système de prévention d'intrusion; 2) Pare-feu/solutions UTM; 3) Saisie intégrale des paquets; 4) Mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et points d'accès (TAP); 7) Surveillance des activités de base de données; 8) Contrôle de l'accès réseau (802.1x); 9) Autres systèmes d'inspection de contenu. Un minimum de trois mois d'expérience est requis dans chaque domaine identifié pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) Certification ISC2 Certified Information System Security Professional (CISSP); 2) Certification ISC2 Certified Cloud Security Professional (CCSP); 3) Certification ISC2 Systems Security Certified Professional (SSCP); et/ou 4) Certification Global Information Assurance Certification (GIAC). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de mandataires comme McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier Trustwave MailMarshall Secure Email Gateway.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la prestation de technologies Cisco, y compris de routeurs et/ou de commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'intégration, de la configuration et de la prestation de technologies Cisco, y compris de routeurs et/ou de commutateurs des séries Nexus et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la résolution de problèmes de pare-feu Palo Alto VM-series.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de générateurs de trafic orientés applications.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de systèmes de détection d'intrusion (IDS).	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 2 à 4 années d'expérience. 2 points : plus de 4 à 6 années d'expérience. 3 points : plus de 6 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la prestation d'équilibreurs de charge F5.	1 point : de 6 mois à 1 année d'expérience 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation de technologies de chiffrement réseau en série.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 22 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de la virtualisation

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de la virtualisation					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie Hyper-V.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation d'un centre de données virtuel.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception de solutions d'infrastructure de postes de travail virtuelle.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la prestation de conseils en matière de sécurité relativement aux infrastructures virtuelles.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'intégration de contrôles de sécurité de tiers au sein d'infrastructures virtuelles.	2 points = 1 projet. 3 points = 2 projets. 4 points = 3 projets ou plus. Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	4		
C8	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la préparation de plans de continuité des activités et de plans de reprise après sinistre ou de la réalisation d'analyses connexes.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
	Total :	**Note de passage minimale : 22 points**	**Note maximale : 32 points**		

C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception architecturale relativement à la solution Stormshield Endpoint Security au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	3 points : plus de 4 à 5 années d'expérience. 4 points : plus de 5 à 6 années d'expérience. 5 points : plus de 6 années d'expérience.	5		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception architecturale relativement à la solution de sécurité Symantec Endpoint Protection au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'application de politiques gouvernementales de sécurité de la TI visant la protection des points d'extrémité au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède d'expérience combinée de l'analyse des éléments suivants : 1) outils et techniques de sécurité de la TI; 2) données de sécurité, présentation d'avis et de rapports concernant celles-ci; 3) statistiques sur la sécurité de la TI.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède d'expérience combinée de la rédaction de rapports techniques, tels que des analyses des exigences, des analyses des options et des documents d'architecture technique.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 à 7 années d'expérience. 4 points : plus de 7 années d'expérience.	4		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Soutien en service, Sécurité nationale des points terminaux (SNPT)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de politiques relatives aux pare-feu au niveau de l'hôte gérés de façon centralisée.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède plus d'une (1) année d'expérience de la prestation d'un soutien technique pour au moins une des technologies de sécurité au niveau de l'hôte suivantes au sein d'un environnement d'entreprise comportant au moins 15000 utilisateurs : 1) Stormshield Endpoint Security; 2) Symantec Endpoint Protection; et 3) McAfee ePolicy Orchestrator.	3 points : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 4 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 5 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	5		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre et du codage des règles F5 Big-IP iRules.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la mise en œuvre de règles relatives à un système de détection des intrusions au niveau de l'hôte géré de façon centralisée.	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinées de la configuration et du soutien des systèmes d'exploitation suivants: 1) Windows 7; 2) Windows Server 2008; et/ou 3) Windows Server 2012.	2 points : d'expérience combinée minimale démontrée pour un (1) des systèmes d'exploitation figurant dans la liste. 3 points : d'expérience combinée minimale démontrée pour deux (2) des systèmes d'exploitation figurant dans la liste. 4 points : d'expérience combinée minimale démontrée pour les trois (3) systèmes d'exploitation figurant dans la liste.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la prestation du soutien de serveurs Syslog.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la tenue à jour de bases de données MS SQL (Microsoft Structured Query Language).	1 point : de 6 mois à 1 année d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 à 3 années d'expérience. 4 points : plus de 3 années d'expérience.	4		
	Total :	**Note de passage minimale : 20 points**	**Note maximale : 29 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de mandataires comme McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier Trustwave MailMarshall Secure Email Gateway.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la conception et de la configuration de la distribution du trafic des applications à l'aide de produits F5 (technologies DNS, LTM et BIGIP).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologie de réseaux Cisco, y compris de protocoles de routage dynamique (p. ex., BGP, OSPF), la séparation de réseaux (p. ex., VRF, VLAN) et la traduction d'adresse réseau (NAT).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C8	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.8 Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience, acquise au cours des dix (10) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : plus de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, en configuration, amélioration et optimisation d'un système de gestion des informations et des événements de sécurité (GIES) dans un environnement de production ou de solutions de saisie intégrale des paquets (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise dans un environnement de 500 à 5 000 utilisateurs. 2 points = expérience acquise dans un environnement de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise dans un environnement de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la prestation de services de détection, d'analyse et de gestion des incidents liés à la sécurité de la TI au moyen d'outils automatisés de GIES.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de l'utilisation et de la configuration de tous les aspects : 1) d'une solution de GIES, y compris la normalisation des données, la transmission des fichiers journaux, le regroupement d'éléments journaux, le stockage des événements et journeaux, l'établissement d'une corrélation entre les fichiers journaux et les événements et la production de rapports et d'alertes; ou 2) d'une solution de saisie intégrale des paquets, y compris la surveillance, la saisie, la collecte, la production et l'analyse de métadonnées.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée a suivi une formation spécifique relative à ArcSight ou à RSA Netwitness ou qu'elle détient une certification relative à la technologie ArcSight ou à la technologie RSA Netwitness.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de l'examen, de l'élaboration et de la mise en œuvre de flux de processus de traitement et d'escalade des incidents dans le cadre d'un projet de GI-TI.	1 point = 1 projet. 2 points = 2 projets. 3 points = 3 projets ou plus. Un minimum de 6 mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource détient au moins l'une des certifications suivantes : 1) International Information System Security Certification Consortium (ISC)^2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA); 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 14 points**	**Note maximale : 20 points**		

PIÈCE JOINTE 4.1

CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 2 – TRÈS SECRET

1. Les critères d'évaluation de la présente pièce jointe serviront à évaluer les soumissions dans le cadre de l'appel d'offres et à faciliter l'évaluation des ressources après l'attribution du contrat.

2. Le soumissionnaire doit fournir un curriculum vitæ admissible pour chaque catégorie de ressources demandée aux fins d'évaluation (le soumissionnaire ne doit pas proposer la même ressource plus d'une fois en réponse au présent appel d'offres).

3. Le soumissionnaire doit remplir une grille d'évaluation pour chacun des curriculum vitæ fournis comme décrit dans le tableau 1 ci-dessous. Pour chaque critère, il doit indiquer la partie du curriculum vitæ où la conformité avec les critères est décrite. À défaut de fournir un curriculum vitæ admissible pour chaque catégorie de ressources, la soumission sera jugée non conforme.

Tableau 1 : Les soumissionnaires doivent soumettre le nombre suivant de curriculum vitæ par catégorie de ressources en réponse à la présente évaluation. Le nombre réel de ressources nécessaire est énuméré au point 1.2 Sommaire de la partie 1 de l'appel d'offres.

Catégorie de ressource et titre de tâche spécifique	Niveau	Nombre de curriculum vitæ
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Gestion de la configuration	3	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Passerelle d'échange d'information	2	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Architecture de référence pour la cybersécurité	3	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Solution interdomaine – Accès	3	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Solution interdomaine – Transfert	2	1
C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones	2	1

C.6 Ingénieur en sécurité de la TI Titre de tâche spécifique : Surveillance de la sécurité des réseaux	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Saisie intégrale des paquets	2	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité de l'hôte	2	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Passerelle d'échange d'information	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Solution interdomaine – Accès	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité de l'hôte	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu	3	1
C.7 Spécialiste en conception de la sécurité de la TI Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité	3	1
C.8 Analyste de la sécurité des réseaux Titre de tâche spécifique : Surveillance de la sécurité des réseaux	3	1
C.8 Analyste de la sécurité des réseaux Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)	3	1
C.12 Spécialiste de la gestion des incidents Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)	3	1

1. EXIGENCES POUR L'ORGANISATION

1.1. Exigences obligatoires pour l'organisation

EXIGENCES OBLIGATOIRES – CRITÈRES POUR L'ORGANISATION			
Point	**Critères obligatoires pour l'organisation**	**RESPECTÉ (oui/non)**	**Numéro de page du document de soumission**
O1	Le soumissionnaire doit s'être fait octroyer au moins deux (2) contrats de service professionnel en informatique† par un client gouvernemental*. Chacun des contrats mentionnés : 1. doit avoir une valeur d'au moins 5 millions de dollars (5 M$), taxes applicables en sus; 2. doit avoir eu une durée d'au moins deux (2) années, doit avoir été octroyé au cours des huit (8) dernières années précédant la date de clôture du présent appel d'offres et n'inclut pas les années d'option qui n'ont pas été exercées; 3. doit montrer que le soumissionnaire a fourni au moins cinq (5) ressources simultanément pendant une période d'au moins douze (12) mois consécutifs. Chacun des contrats mentionnés doit également montrer que le soumissionnaire a fourni des services à une organisation dans un milieu : • doté d'au moins 100 postes de travail connectés à un réseau protégé ou secret; • utilisant des systèmes d'exploitation Windows pour poste de travail (Windows XP, Windows Vista, Windows 7 ou Windows 10); • faisant appel à une gestion centralisée de la distribution de logiciels et des correctifs. Le soumissionnaire doit fournir une (1) référence pour chaque contrat. Chaque preuve de références doit inclure le nom de l'organisation, le numéro d'identification unique du contrat, une brève description des services fournis, le nom, le titre, l'adresse électronique et le numéro de téléphone du cadre responsable de l'organisation, le nombre de ressources fournies, ainsi que la date d'attribution, la date de fin et la valeur (en dollars) de chaque contrat. Il incombe au soumissionnaire de s'assurer que tout renseignement est		

	divulgué avec la permission des références fournies. Le soumissionnaire doit avoir été l'entrepreneur principal, et non un sous-traitant. Autrement dit, le soumissionnaire a passé un contrat directement avec le client. Si le contrat du soumissionnaire prévoyait qu'il devait effectuer des travaux pour lesquels les services d'une autre entité avaient d'abord été retenus par contrat, le soumissionnaire ne serait pas considéré comme l'entrepreneur principal. Par exemple, Z (le client) attribue un contrat de services à Y. Y, à son tour, passe un contrat avec X pour fournir une partie ou la totalité de ces services à Z. Dans cet exemple, Y est l'entrepreneur principal et X est le sous-traitant. Le soumissionnaire doit se rappeler qu'un arrangement en matière d'approvisionnement (AMA) ou une offre à commandes ne constitue pas un contrat et que, par conséquent, toute référence à ce type de documents sera exclue du processus d'évaluation de l'expérience du soumissionnaire en matière d'exécution de contrats. Par exemple, si le soumissionnaire cite en référence son numéro d'AMA des Services professionnels en informatique centrés sur les tâches (SPICT), tel que EN578-055605/XXX/EL, en guise de preuve de l'expérience aux termes des critères d'évaluation, le Canada ne tiendra pas compte de cette expérience, car elle ne se rapporte pas à un contrat particulier. *Client gouvernemental s'entend d'un ministère ou d'un organisme fédéral, provincial ou municipal ou d'une société d'État. † Les « services professionnels en informatique » sont des services professionnels fournis par le soumissionnaire à l'appui d'un projet ou d'un marché en technologie ou en gestion de l'information.		

CRITÈRES LIÉS AUX RESSOURCES

CRITÈRES OBLIGATOIRES

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de la configuration

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de la configuration				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la planification et de la mise en œuvre de solutions de sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de l'exécution des tâches liées à la conception de l'architecture de sécurité ou au soutien en ingénierie dans le domaine de la sécurité de la TI.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée, au cours des dix (10) dernières années, de la planification, de l'élaboration, de la mise en œuvre et de l'intégration de solutions d'évaluation de la vulnérabilité.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de l'élaboration et de la mise en œuvre d'un programme de gestion des vulnérabilités pour une organisation comptant au moins 5 000 utilisateurs.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'application des politiques de sécurité de la TI du gouvernement.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées à un serveur mandataire Web.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration de solutions de service de protection des limites de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations; • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Architecture de référence pour la cybersécurité

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Architecture de référence pour la cybersécurité				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de la planification et/ou de la mise en œuvre des services de technologie de l'information, tels que les services Web, les services de bases de données, les services d'annuaire, les services d'accès utilisateurs, les environnements virtuels et/ou les postes de travail virtuels.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'examen, de la conception, de la planification et/ou de la mise en œuvre de services de sécurité ou de l'architecture de sécurité des systèmes de TI soutenant plus d'une centaine d'utilisateurs.			
O3	Le soumissionnaire doit démontrer que la ressource proposée a acquis au moins cinq (5) années d'expérience de la rédaction de documents techniques de configuration ou de mise en œuvre.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de l'élaboration, de la configuration et de la mise à l'essai de contrôles et de politiques de sécurité de réseau.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception et de la prestation de services de postes de travail virtuels.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception, de la configuration et de la mise en œuvre de modèles de contrôle d'accès fondés sur les rôles et sur des règles.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • les spécifications de la conception du système; • les documents sur la construction et la configuration; • le concept d'opérations (ConOp); • les plans de mise en œuvre de systèmes; • les plans d'essais et les rapports de mises à l'essai; et • les plans de soutien du cycle de vie.			
O6	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception, de la configuration et de la mise en œuvre de modèles de canal sécurisé IPSec.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Solution interdomaine – Transfert

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Solution interdomaine – Transfert				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies 'High Assurance Guard'.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration des technologies de filtre de contenu de courriel (comme la protection contre les logiciels malveillants) et de prévention de la perte de données (par exemple, le contrôle de label et la vérification du vocabulaire).			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • les spécifications de la conception du système; • les documents sur la construction et la configuration; • le concept d'opérations (CONOP); • les plans de mise en œuvre de systèmes; • les plans d'essais et les rapports de mises à l'essai; • les plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux pare-feu.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies liées aux serveurs mandataires Web.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de la configuration et de l'intégration des technologies d'agent de transfert de courrier.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'ingénierie, de la conception, de la configuration et de l'intégration de solutions de service de protection des limites de réseau.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'ingénieur en sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée de la rédaction et de la tenue à jour de la documentation technique et d'ingénierie sur la gestion des informations et des événements de sécurité (SIEM) et la saisie intégrale des paquets (Full Packet Capture).			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la surveillance de la sécurité des réseaux dans un environnement de déploiement d'entreprise.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des dix (10) dernières années, de la conception, du déploiement et de l'intégration des outils de GIES (SIEM) ou de la saisie intégrale des paquets dans un environnement de production.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Saisie intégrale des paquets

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Saisie intégrale des paquets				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de la conception, du déploiement, de l'administration ainsi que de la résolution de problèmes de composants de l'infrastructure de communication du réseau local ou étendu.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de l'administration du système Linux ou d'une variante de Linux.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité de l'hôte

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité de l'hôte				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, à titre de spécialiste en conception de sécurité de la TI.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée, acquise au cours des sept (7) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de capacités de sécurité visant à protéger les points d'extrémité dans un environnement de TI d'entreprise. L'expérience relative logiciels de sécurité pour la protection des points d'extrémité doit comprendre deux (2) des éléments suivants : antivirus, prévention de la perte de données (PPD), balisage de données, la gestion des droits liés aux données d'entreprise, logiciel Endpoint detection and response (EDR), pare−feu hôte, analyse et ingénierie inverse des logiciels malveillants, contrôle des applications, prévention des intrusions au niveau de l'hôte, balisage et protection des données, analytique des comportements des utilisateurs et des entités (UEBA), chiffrement intégral de disque et chiffrement de supports amovibles.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de protection des points d'extrémité de sécurité de la TI dans un environnement de TI d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de la rédaction d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de construction et de configuration; • concept d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'élaboration d'une conception d'architecture de sécurité pour une solution classifiée du gouvernement (dont la classification est « Secret » ou supérieure).			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'utilisation d'au moins un (1) des procédés ou cadres architecturaux suivants : • TOGAF (The Open Group Architecture Framework); • FEAP (gouvernement américain); • Programme de transformation opérationnelle du gouvernement du Canada; • Zachman; ou • Cadre d'architecture de sécurité SABSA (Sherwood Applied Business Security Architecture Institute)			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des sept (7) dernières années, de l'analyse d'exigences, de la conception et de la mise en œuvre des exigences relatives à la solution de GIJIA.			
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience de la prestation de séances d'information à l'intention des cadres supérieurs (niveaux des directeurs et niveaux supérieurs) relatives aux considérations en matière de sécurité de la TI et aux mesures recommandées.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai et de la tenue à jour de l'équipement des technologies sécurité de réseau suivant et de la résolution de problèmes connexes : • sentinelles et passerelles; • pare-feu; • service de protection des limites de réseau; • diodes de données; • serveurs mandataires Web; • agent de transfert de courrier. La ressource proposée doit posséder au moins deux (2) années d'expérience relativement à chacune des technologies susmentionnées.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée de la conception, de l'ingénierie, de l'installation, de la configuration, de la mise à l'essai et de la tenue à jour des produits et infrastructures de TI suivants et de la résolution de problèmes connexes : • système d'exploitation en réseau Microsoft; • réseaux IP; • intégration d'applications; • virtualisation. La ressource proposée doit posséder au moins trois (3) années d'expérience relativement à chacune des technologies susmentionnées.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; et • plans de soutien du cycle de vie.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des six (6) dernières années, de l'utilisation de réseaux classifiés communs au niveau « Secret » ou « Très secret ».			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la planification et de la mise en œuvre d'architectures d'intégration de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience de la conception et de la mise en œuvre de contrôles et de politiques de sécurité de réseau ainsi que de la gestion du changement à cet égard.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de services de postes de travail virtuels ainsi que de la gestion du changement à cet égard.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de modèles de contrôle d'accès fondés sur les rôles et sur des règles ainsi que de la gestion du changement à cet égard.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de modèles de canal sécurité IPSec ainsi que de la gestion du changement à cet égard.			
O6	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée de l'élaboration d'au moins trois (3) des types de documents sur l'ingénierie des systèmes suivants : • spécifications de conception de système; • documents de conception et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de l'hôte

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de l'hôte				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience de la conception et de la mise en œuvre de solutions de sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la conception, de l'ingénierie, de l'installation, de la configuration et de la mise à l'essai de logiciels de sécurité visant à protéger les points d'extrémité dans un environnement de TI d'entreprise. L'expérience relative logiciels de sécurité pour la protection des points d'extrémité doit comprendre trois (3) des éléments suivants : antivirus, prévention de la perte de données (PPD), balisage de données, gestion des droits liés aux données d'entreprise, logiciel Endpoint detection and response (EDR), pare-feu hôte, analyse et ingénierie inverse des logiciels malveillants, contrôle des applications, prévention des intrusions au niveau de l'hôte, balisage et protection des données, analytique des comportements des utilisateurs et des entités (UEBA), chiffrement intégral de disque et chiffrement de supports amovibles.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de l'application des politiques de protection des points d'extrémité de sécurité de la TI dans un environnement de TI d'entreprise.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience combinée dans l'élaboration d'au moins trois (3) différents types de documents sur l'ingénierie des systèmes suivants: • spécifications de conception de système; • documents de construction et de configuration; • concepts d'opérations (CONOP); • plans de mise en œuvre de systèmes; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience, acquise au cours des dix (10) dernières années, de la configuration et de l'intégration d'équipement de réseau.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des dix (10) dernières années, de la conception d'architectures sécurisées en respectant les lignes directrices énoncées dans les documents *Conseils en matière de sécurité des technologies de l'information* (ITSG-22, ITSG-33 et ITSG-38) du Centre de la sécurité des télécommunications.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience, acquise au cours des huit (8) dernières années, de la configuration, de l'intégration et de la résolution de problèmes de pare-feux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience de l'intégration de validations de principe relatives à des solutions de sécurité de la TI.			
	Conforme (oui/non)?			

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste en conception de la sécurité de la TI.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de l'élaboration et de la mise en œuvre d'une solution axée sur la gouvernance d'entreprise, la gestion des risques et la conformité pour une organisation comptant au moins 5 000 utilisateurs.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de l'évaluation des contrôles de sécurité, de l'évaluation de la menace et des risques associés à un système de TI ou de l'interprétation et de l'application des lignes directrices énoncées à l'annexe A des *Conseils en matière de sécurité des technologies de l'information (ITSG) 33*.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des dix (10) dernières années, de la définition des exigences, de la transformation des processus opérationnels en un flux des travaux et de l'ingénierie de solutions aux stades de la définition et de la mise en œuvre d'un projet de sécurité de la TI.			
	Conforme (oui/non)?			

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comptant au moins 500 utilisateurs.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la collecte et de l'analyse de codes malveillants des hôtes et du trafic sur le réseau.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée, acquise au cours des huit (8) dernières années, de la surveillance, de la configuration et de la mise au point d'outils GIES ou de la saisie intégrale des paquets dans un environnement de production.			
	Conforme (oui/non)?			

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre d'analyste de la sécurité des réseaux.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des cinq (5) dernières années, de la configuration et de la prestation d'un soutien technique pour l'outil de gestion des informations et des événements de sécurité (GIES) ArcSight dans un environnement de production.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la surveillance et de l'analyse de fichiers journaux de sécurité pour un réseau d'entreprise comptant au moins 500 utilisateurs.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la GIES pour les serveurs et les postes de travail dans un environnement de déploiement d'entreprise.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception, de la configuration et de la résolution de problèmes de serveurs Linux.			
	Conforme (oui/non)?			

C.12 – Spécialiste de la gestion des incidents – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
C.12 – Spécialiste de la gestion des incidents de niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)				
O1	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience, acquise au cours des quinze (15) dernières années, à titre de spécialiste de la gestion des incidents.			
O2	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience, acquise au cours des six (6) dernières années, de la mise en œuvre et de la prestation de soutien technique pour l'outil de gestion des informations et des événements de sécurité (GIES) ArcSight dans un environnement de production.			
O3	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception et de la mise en œuvre de scénarios d'utilisation de la GIES pour les serveurs et les postes de travail dans un environnement de déploiement d'entreprise.			
O4	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la conception, de la configuration et de la résolution de problèmes de serveurs Linux.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (EMPLACEMENT DANS LA PROPOSITION, CRITÈRE NON RESPECTÉ, ETC.)
O5	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience de la création et de la tenue à jour de documents ou de produits livrables d'ingénierie sur la GIES.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de la configuration

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de la configuration					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'application des politiques du gouvernement en matière de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'analyse des options relatives aux outils et aux techniques de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la planification, de l'élaboration, de la mise en œuvre et de l'intégration des solutions de détection de biens de TI et de base de données de gestion de la configuration (BDGC).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la planification, de l'élaboration, de la mise en œuvre et de l'intégration de solutions automatisées de vérification de la conformité des configurations.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la rédaction de rapports techniques comme les documents d'analyse des exigences, d'analyse des options et d'architecture technique.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'élaboration de guides de renforcement de la sécurité des systèmes de TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1. Certified Information System Security Professional (CISSP); 2. Systems Security Certified Practitioner (SSCP); 3. GIAC Security Essentials (GSEC); 4. Microsoft Certified Solutions Expert (MCSE); 5. Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 19 points**	**Note maximale : 27 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de serveurs mandataires, comme le McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier pour la passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Architecture de référence pour la cybersécurité

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Architecture de référence pour la cybersécurité					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de la conception, de façon individuelle ou conjointe, d'un environnement de TI à grande échelle pour au moins 100 utilisateurs.	Soutien pour les utilisateurs de la TI 3 points : de 100 à 300 utilisateurs. 4 points : de 300 à 1 000 utilisateurs. 5 points : 1 000 utilisateurs et plus.	5		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la mise en application des processus de gestion des risques pour la sécurité de la TI ou des processus d'ingénierie pour la sécurité des systèmes.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de méthodes de détection d'intrusion de la TI et de protection contre l'intrusion de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de solutions de surveillance de système axée sur les accès, les changements ou l'état de fonctionnement.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration de services de TI d'entreprise, notamment les services de répertoire, d'authentification unique, de courriel, de sauvegarde ou de base de données distribuée pour un système de TI utilisé par au moins 500 utilisateurs.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la conception ou de la mise en œuvre et de la configuration des principes de défense en profondeur de la TI. Le soumissionnaire doit démontrer la façon dont la ressource a mis en application ces principes et en fournir une description.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'utilisation d'un cadre d'architecture d'entreprise reconnu.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C8	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la rédaction de documents techniques destinés à un personnel organisationnel à l'aide des outils bureautiques.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 4 années d'expérience. 3 points : plus de 4 à 6 années d'expérience. 4 points : plus de 6 années d'expérience.	4		
	Total :	**Note de passage minimale : 19 points**	**Note maximale : 27 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Solution interdomaine – Transfert

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Solution interdomaine – Transfert					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 2
Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 2 Titre de tâche spécifique : Passerelle d'échange d'information et établissement de zones					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de serveurs mandataires, comme le McAfee Web Gateway, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions d'agent de transfert de courrier pour la passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de solutions VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine (DNS).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la mise en œuvre de Red Hat Enterprise Linux (RHEL).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 17 points**	**Note maximale : 24 points**		

C.6 – Ingénieur en sécurité de la TI – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.6 – Ingénieur en sécurité de la TI – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, de l'expérience dans l'ingénierie de solutions de surveillance de la sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité suivantes : 1) sécurité au niveau de l'hôte; 2) système de détection d'intrusion et système de prévention d'intrusion (IDS/IPS); 3) pare-feu et produits de gestion unifiée des menaces (UTM); 4) saisie intégrale des paquets 5) serveurs mandataires; 6) équilibreurs de charge; 7) commutateurs matriciels et prises réseau (Taps).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	Le soumissionnaire devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou sur la plateforme RSA Netwitness ou qu'elle détient une certification à jour sur la technologie ArcSight ou la technologie RSA Netwitness. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, de l'expérience dans la conception de solutions de surveillance de la sécurité des réseaux pour le gouvernement s'appuyant sur les directives de sécurité des TI (DSTI) 02 ou les conseils en matière de sécurité des TI (ITSG) 22 au niveau « Protégé B » ou supérieur.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la prestation de services d'ingénierie de sécurité de la TI pour des ministères et des organismes du gouvernement sous forme de développement d'architecture de sécurité, de conseils et de directives connexes.	1 point : de 3 à 5 années d'expérience. 2 points : plus de 5 à 7 années d'expérience. 3 points : plus de 7 à 9 années d'expérience. 4 points : plus de 9 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1) International Information System Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH) 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux http://www.cicic.ca/1/accueil.canada	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 16 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Saisie intégrale des paquets

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Saisie intégrale des paquets					
C1	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception, la planification et la mise en œuvre d'une infrastructure de réseau d'environnements complexes et hautement accessibles*. *On entend par « environnements complexes et hautement accessibles », des environnements qui touchent plusieurs villes ou pays et pour lesquels aucun temps d'interruption de service n'est permis.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, d'expérience combinée dans la réalisation d'au moins une des activités de TI suivantes : 1. Rédaction de rapports techniques comme les documents d'analyse des exigences, d'analyse des options, d'artéfacts de processus d'ingénierie ou de l'architecture technique; 2. Automatisation de l'administration des systèmes Linux au moyen de scripts et d'interfaces de programmation d'applications comme les langages Ruby, PHP, Bash, Perl ou Python; 3. Analyse des données brutes relatives au trafic sur le réseau à l'appui de la résolution de problèmes ou de l'analyse judiciaire des réseaux; 4. Déploiement et administration de dispositifs de surveillance du trafic du réseau ou d'analyse judiciaire des réseaux comme FireEye, Solera, Sourcefire et Cisco, système de détection ou de prévention d'intrusion, SNORT ou Netwitness (RSA Security Analytics); 5. Examen des alertes et des paquets provenant de capteurs de détection d'intrusion (IDS) ou de dispositifs de saisie des paquets;	1 point : de 6 à 9 mois d'expérience. 2 points : plus 9 à 12 mois d'expérience. 3 points : plus 12 à 15 mois d'expérience. 4 points : plus 15 mois d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	6. Analyse de logiciels malveillants et analyse de type bac à sable à l'aide d'applications comme Netwitness Spectrum et RSA Malware, WireShark, CaptureBAT ou Cuckoo Sandbox et la capacité d'ingénierie inversée et de débogage des logiciels malveillants à l'aide d'outils comme IDA Pro, Responder Pro ou OllyDbg, y compris des techniques de défense contre l'antidébogage, l'élaboration de trousses et le brouillage. 7. Gestion des technologies de réseau de stockage (SAN) et NAS – canal de fibre optique, FCOE (canal de fibre optique sur réseau Ethernet), iSCSI (interface de système pour microordinateur sur Internet), serveur NFS (système de fichiers en réseau), protocole CIFS, notamment des numéros d'unité logique, le câblage, la résolution de problèmes et les correctifs. Un minimum de trois (3) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.				

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource détient au moins l'une des certifications en sécurité de la TI suivantes : 1) RSA Security Analytics Certified Administrator; 2) Toute certification Cisco de niveau « Associé »; 3) Toute certification Cisco de niveau « Professionnel »; 4) Toute certification Cisco de niveau « Expert »; 5) Toute certification GIAC du SANS institute dans la catégorie « Security Administration »; 6) Toute certification Red Hat Certified System Administrator, Red Hat Certified Engineer ou Red Hat Certified Architect. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 certifications ou plus.	5		
	Total :	**Note de passage minimale : 8 points**	**Note maximale : 12 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2
Titre de tâche spécifique : Sécurité de l'hôte

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 2 Titre de tâche spécifique : Sécurité de l'hôte					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins un (1) an d'expérience de l'application de politiques de protection des points d'extrémité de sécurité de la TI du gouvernement dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte géré de façon centralisée dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte de McAfee, Symantec ou Trend-Micro dans un environnement de TI d'entreprise.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'ingénierie et de la mise en œuvre de chacune des technologies de sécurité au niveau de l'hôte dans un environnement de TI d'entreprise suivantes : 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; 3) 3) Trend-Micro Control Manager.	1 point : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 2 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 3 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de l'intégration ou du soutien des logiciels de gestion de McAfee, Symantec ou Trend-Micro pour les environnements virtuels optimisés dans un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'évaluation de diverses technologies de sécurité de la TI et de la documentation d'une analyse aux fins de prise de décision de la direction.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie et de la mise en œuvre de solutions de sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité des réseaux suivantes : 1) système de détection d'intrusion et système de prévention d'intrusion (IDS/IPS); 2) pare-feu et produits de gestion unifiée des menaces (UTM); 3) Saisie intégrale des paquets; 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prise réseaux (Taps); 7) Surveillance de l'activité de la base de données; 8) Contrôle de l'accès au réseau (802.1x); 9) Autres systèmes d'inspection de contenu Un minimum de trois (3) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); 4) Toute certification Global Information Assurance Certification (GIAC). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 certifications ou plus.	5		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 26 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et Infrastructure à clé publique (ICP)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration de procédures opérationnelles normalisées (PON) pour des projets.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception et le déploiement de technologies liées aux ICP.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception et le déploiement de solutions de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de la conception de solutions de TI qui nécessitent une interopérabilité avec les systèmes : • d'un ou plusieurs ministères du gouvernement du Canada; ou • d'un ou plusieurs des partenaires internationaux suivants : les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.	1 point : expérience d'au moins six (6) mois démontrée dans la conception de solutions de TI qui exigent une interopérabilité avec les systèmes des ministères du gouvernement du Canada. 2 points : expérience d'au moins six (6) mois démontrée dans la conception de solutions de TI qui exigent l'interopérabilité avec les systèmes de partenaires internationaux (États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande)	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la conception de schémas de processus pour un concept d'architecture de sécurité.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Passerelle d'échange d'information

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Passerelle d'échange d'information					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de pare-feu, comme McAfee, Palo Alto ou F5.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre des technologies de serveurs mandataires, comme la passerelle Web McAfee, F5 ou Blue Coat.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de solutions de passerelle de courriel sécurisé de Trustwave (anciennement MailMarshal) et d'agent de transfert de courrier.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de technologies de protocoles SSL, HTTPS, HTTP, IPSec et SMTP.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède de l'expérience de la configuration, de l'intégration et de la mise en œuvre de la technologie VMware.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine au sein de grands réseaux de TI (comptant au moins 1 000 utilisateurs).	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution des technologies de réseautage Cisco, y compris les routeurs et les commutateurs.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Solution interdomaine – Accès

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Solution interdomaine – Accès					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'application des politiques de sécurité de la TI du gouvernement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède d'expérience combinée de la réalisation des trois (3) tâches de sécurité des TI suivantes : 1) analyse des outils et des techniques de sécurité de la TI; 2) analyse des données de sécurité et présentation d'avis et de rapports; 3) rédaction de rapports techniques, y compris les documents d'analyse des exigences, d'analyse des options, d'architecture technique et de modélisation des risques mathématiques; 4) conception de l'architecture de sécurité et soutien d'ingénierie; 5) études liées à la classification de la sécurité des données. Un minimum de six (6) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la mise en œuvre de Windows Server 2008 (ou d'une version plus récente), d'Active Directory et du système de noms de domaine.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la conception et de la mise en œuvre et de la gestion du changement liées aux technologies VMWare	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins l'une des certifications suivantes dans le domaine de l'architecture : 1) Certification TOGAF (The Open Group Architecture Framework) 2) Certification en Gestion des services en technologie de l'information (GSTI) 3) Certification du EACOE (Enterprise Architecture Center of Excellence) 4) Certification Microsoft Certified Architect (MCA); 5) Certification VMware Certified Design Expert (VCDX). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 11 points**	**Note maximale : 15 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de l'hôte

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de l'hôte					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'application de politiques de protection des points d'extrémité de la sécurité de la TI du gouvernement dans un environnement de TI d'entreprise.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité au niveau de l'hôte géré de façon centralisée dans un environnement de TI d'entreprise.	1 point : de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la mise en œuvre de politiques de sécurité des points d'extrémité sur un hôte McAfee dans un environnement de TI d'entreprise.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins une (1) année d'expérience de l'ingénierie et de la mise en œuvre pour chacune des technologies de sécurité au niveau de l'hôte dans un environnement de TI d'entreprise suivantes : 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; 3) 3) Trend-Micro Control Manager.	1 point : expérience minimale démontrée pour une (1) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 2 points : expérience minimale démontrée pour deux (2) des technologies de sécurité au niveau de l'hôte figurant dans la liste. 3 points : expérience minimale démontrée pour les trois (3) technologies de sécurité au niveau de l'hôte figurant dans la liste.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie, de l'intégration ou du soutien des logiciels de gestion de McAfee, Symantec ou Trend-Micro pour les environnements virtuels optimisés dans un environnement de production.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 années d'expérience.	2		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une l'expérience de l'évaluation de diverses technologies de sécurité de la TI et de la documentation d'une analyse aux fins de prise de décision de la direction.	1 point par projet jusqu'à un maximum de trois (3) projets*† * Si un soumissionnaire fournit plus de trois (3) projets en réponse à ce critère, seuls les trois (3) premiers projets cités seront évalués. †Un minimum de six (6) mois d'expérience par projet est requis pour que le projet soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'ingénierie et de la mise en œuvre de solutions de sécurité des réseaux à l'aide d'au moins trois (3) des technologies de sécurité des réseaux suivantes : 1) SDI/SPI 2) Pare-feu et produits UTM; 3) Saisie intégrale des paquets; 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseau (Taps); 7) Surveillance de l'activité de la base de données; 8) Contrôle de l'accès au réseau (802.1x); 9) Autres systèmes d'inspection de contenu Un minimum de six (6) mois d'expérience est requis dans chaque domaine indiqué pour que l'expérience soit prise en compte.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 à 4 années d'expérience. 4 points : plus de 4 années d'expérience.	4		
	Total :	**Note de passage minimale : 15 points**	**Note maximale : 21 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Sécurité de réseaux – Inspection de contenu					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution de technologies Cisco, y compris les routeurs ou les commutateurs de série NEXUS et Catalyst.	1 point : de 5 à 6 années d'expérience. 2 points : plus de 6 à 7 années d'expérience. 3 points : plus de 7 à 8 années d'expérience. 4 points : plus de 8 années d'expérience.	4		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration ainsi que de la résolution de problèmes de solutions de pare-feu Palo Alto.	1 point : de 3 à 4 années d'expérience. 2 points : plus de 4 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'utilisation d'outils de génération de trafic en fonction de l'application.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'utilisation de systèmes de détection d'intrusion (IDS).	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'utilisation de VMWare.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la configuration, de l'intégration et de la distribution des équilibreurs de charge F5.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'utilisation des technologies de chiffrement de réseau en série.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP) 3) GIAC Security Essentials (GSEC) 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 18 points**	**Note maximale : 25 points**		

C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3
Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.7 – Spécialiste en conception de la sécurité de la TI – Niveau 3 Titre de tâche spécifique : Gouvernance d'entreprise, risques et conformité					
C1	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins l'une des certifications suivantes dans le domaine de l'administration des applications axées sur la gouvernance, la gestion des risques et la gestion de la conformité de TI ou d'entreprise : 1) RSA Archer Certified Administrator; 2) IBM OpenPages Administrator ; 3) MetricStream GRC Certified Administrator . Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C2	Le soumissionnaire devrait démontrer que la ressource proposée a acquis au cours des cinq (5) dernières années, d'expérience combinée dans la création de transformation de données XML ou de scripts de traduction.	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience.	3		
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience des projets de conception de sécurité de la TI dans un environnement de mise en œuvre d'un cadre de gouvernance, de gestion des risques et de conformité d'entreprise (eGRC).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'application des politiques du gouvernement en matière de sécurité de la TI.	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C6	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, d'expérience combinée dans l'accréditation d'un système de TI au moyen du processus d'évaluation de sécurité et autorisation (SA&A) ou du programme de certification et d'accréditation (C&A).	1 point : de 1 à 2 années d'expérience. 2 points : plus de 2 à 3 années d'expérience. 3 points : plus de 3 années d'expérience.	3		
C7	Le soumissionnaire devrait démontrer que la ressource proposée a acquis, au cours des sept (7) dernières années, de l'expérience dans l'élaboration des architectures de sécurité de réseau (niveau II ou supérieur) s'appuyant sur les directives de sécurité de la TI (DSTI) ou sur les *Conseils en matière de sécurité des technologies de l'information* (ITSG).	1 point : de 6 mois à 1 an d'expérience. 2 points : plus de 1 à 2 années d'expérience. 3 points : plus de 2 années d'expérience	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C8	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins une des certifications en sécurité de la TI suivantes : 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP) 3) GIAC Security Essentials (GSEC) 4) Microsoft Certified Solutions Expert (MCSE); 5) Cisco Certified Network Associate (CCNA). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		
	Total :	**Note de passage minimale : 16 points**	**Note maximale : 23 points**		

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Surveillance de la sécurité des réseaux

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Surveillance de la sécurité des réseaux					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience, acquise au cours des dix (10) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, aux tâches portant sur la configuration, l'amélioration et l'optimisation de solutions de gestion des informations et des événements de sécurité (GIES) ou de solutions de saisie intégrale des paquets (à l'exclusion des environnements de laboratoire) dans un environnement de production pour une grande organisation.	1 point = expérience acquise; soutien de 500 à 5 000 utilisateurs. 2 points = expérience acquise; soutien de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise; soutien de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de la prestation de services de détection, d'analyse et de gestion des incidents liés à la sécurité de la TI au moyen d'outils automatisés de GIES.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience.	3		
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'exécution et de la configuration de tous les volets d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre journaux et événements, et la production de rapports et d'alertes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C5	Le soumissionnaire devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou sur la plateforme RSA Netwitness ou qu'elle détient une certification à jour sur la technologie ArcSight ou la technologie RSA Netwitness. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience de l'examen, de l'élaboration et de la mise en œuvre de flux de processus de traitement et d'escalade d'incidents dans le cadre d'un projet de gestion de l'information et de technologie de l'information.	1 point – 1 projet. 2 points – 2 projets. 3 points – 3 projets ou plus. Un minimum de six (6) mois d'expérience est requis pour chaque projet afin qu'il soit pris en compte.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée détient au moins l'une des certifications en sécurité de la TI suivantes : 1) International Information System Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission. Les certifications doivent avoir été obtenues auprès d'un établissement agréé reconnu par le Centre d'information canadien sur les diplômes internationaux (http://www.cicic.ca/1/accueil.canada).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications ou plus.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
	Total :	**Note de passage minimale : 14 points**	**Note maximale : 20 points**		

C.8 – Analyste de la sécurité des réseaux – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.8 – Analyste de la sécurité des réseaux – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la surveillance de la sécurité des réseaux et de l'analyse des journaux pour détecter les activités malveillantes.	1 point : plus de 2 à 3 années d'expérience. 2 points : plus de 3 à 4 années d'expérience. 3 points : plus de 4 années d'expérience	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue de la réalisation d'un projet portant sur la configuration, l'amélioration et la tenue à jour de solutions de gestion des informations et des événements de sécurité (GIES) dans un environnement de production (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise; soutien de 500 à 5 000 utilisateurs. 2 points = expérience acquise; soutien de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise; soutien de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la prestation d'un soutien technique pour au moins trois (3) des technologies de sécurité de réseau suivantes : 1) Sécurité au niveau de l'hôte; 2) Système de détection d'intrusion et système de prévention d'intrusion (SDI/SPI); 3) Pare-feu et produits de gestion unifiée des menaces (UTM); 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseaux (Taps).	1 point : de 2 à 5 mois d'expérience. 2 points : plus de 5 mois d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience du déploiement et de l'exécution de tous les aspects d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre les journaux et les événements, et la production de rapports et d'alertes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'amélioration et de la configuration des composants de la GIES afin d'en accroître l'efficacité, la précision et le rendement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de travail, acquise au cours des sept (7) dernières années, dans un environnement de soutien des services internes et de centre d'assistance.	1 point : de 1 à 6 mois d'expérience. 2 points : plus de 6 mois d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou qu'elle détient une certification à jour relative à la technologie ArcSight. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
	Total :	**Note de passage minimale : 13 points**	**Note maximale : 18 points**		

C.12 – Spécialiste de la gestion des incidents – Niveau 3
Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C.12 – Spécialiste de la gestion des incidents – Niveau 3 Titre de tâche spécifique : Gestion des informations et des événements de sécurité (GIES)					
C1	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la réalisation d'activités de surveillance de la sécurité des réseaux et de l'analyse de journaux pour détecter les activités malveillantes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C2	Le soumissionnaire devrait démontrer que la ressource proposée possède au moins six (6) mois d'expérience continue dans un projet, travaillant à la configuration, l'amélioration et la tenue à jour de solutions de gestion des informations et des événements de sécurité (GIES) dans un environnement de production (à l'exclusion des environnements de laboratoire) pour une grande organisation.	1 point = expérience acquise dans un environnement de 500 à 5 000 utilisateurs. 2 points = expérience acquise dans un environnement de 5 000 à 10 000 utilisateurs. 3 points = expérience acquise dans un environnement de plus de 10 000 utilisateurs.	3		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C3	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience, acquise au cours des sept (7) dernières années, de la prestation d'un soutien technique pour au moins trois (3) des technologies de sécurité de réseau suivantes : 1) Sécurité au niveau de l'hôte; 2) Système de détection d'intrusion et système de prévention d'intrusion (SDI/SPI); 3) Pare-feu et produits de gestion unifiée des menaces (UTM); 4) Serveurs mandataires; 5) Équilibreurs de charge; 6) Commutateurs matriciels et prises réseau (Taps).	1 point : de 2 à 5 mois d'expérience. 2 points : plus de 5 mois d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C4	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience du déploiement et de l'exécution de tous les aspects d'une solution de GIES, y compris : la normalisation des données, la transmission de journaux, le regroupement des journaux, le stockage des journaux et des événements, la corrélation entre les journaux et les événements, et la production de rapports et d'alertes.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C5	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de l'amélioration et de la configuration des composants de la GIES afin d'en accroître l'efficacité, la précision et le rendement.	1 point : de 1 à 3 années d'expérience. 2 points : plus de 3 à 5 années d'expérience. 3 points : plus de 5 années d'expérience.	3		
C6	Le soumissionnaire devrait démontrer que la ressource proposée possède une expérience de travail, acquise au cours des sept (7) dernières années, dans un environnement de soutien des services internes et de centre d'assistance.	1 point : de 1 à 6 mois d'expérience. 2 points : plus de 6 mois d'expérience.	2		

Nº	CRITÈRES	GUIDE DE COTATION	NBRE MAX. DE POINTS	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)
C7	Le soumissionnaire devrait démontrer que la ressource proposée a suivi une formation spécialisée sur ArcSight ou qu'elle détient une certification à jour relative à la technologie ArcSight. Une copie de la certification ou des certifications valides détenues par la ressource (ou le numéro d'identification des certifications en cause accompagné d'un lien Web permettant d'en vérifier la validité) doit être fournie avec la soumission.	1 point = 1 certification. 2 points = 2 certifications ou plus.	2		
	Total :	**Note de passage minimale : 13 points**	**Note maximale : 18 points**		