

d Travaux publics et vices Services gouvernementaux Canada

RETURN BIDS TO:

Bid Receiving - PWGSC / Réception des soumissions – TPSGC

RETOURNER LES SOUMISSIONS À:

11 Laurier St. / 11, rue Laurier Place du Portage, Phase III Core 0B2 / Noyau 0B2 Gatineau Quebec K1A0S5

Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution

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		Amendment No N° modif.		
W6369-17P5LA/A		007		
Client Reference No N° de réfe	érence du client	Date		
W6369-17P5LA		2018-11-02		
GETS Reference No N° de réfé	érence de SEAG			
PW-\$IPS-004-33815				
File No N° de dossier	CCC No./N° CCC - FMS	No./N	N° VME	
004ips.W6369-17P5LA				
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2018-11-09				
F.O.B F.A.B. Specified He	erein - Précisé dans les pr	résente	es	
Plant-Usine: Destination:	Other-Autre:			
Address Enquiries to: - Adresse	er toutes questions à:		Buyer Id - Id de l'acheteur	
Patel, Ankoor			004ips	
Telephone No N° de téléphone	•	FAX I	No N° de FAX	
(613) 858-9403 ()		()	-	
Destination - of Goods, Service: Destination - des biens, service				

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigee	Delivery Offered - Livraison proposee
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 sig (type or print) Nom et titre de la personne autorisée à sig de l'entrepreneur (taper ou écrire en carac	gner au nom du fournisseur/
Signature	Date



Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

MODIFICATION NO 007

La présente modification vise à modifier la demande de propositions (DP) et à répondre aux questions des soumissionnaires.

MODIFICATIONS À LA DDP:

1. Enlever: Section 7.5 Volet de travail 1 – Secret, de (a) à (k) ; et

Remplacer par:

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN: DOSSIER TPSGC # W6369-17-P5LA S1 Révision # 1

- (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 NATO 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 CLASSIFIÉS/ PROTÉGÉS RESTREINTS, ou à des établissements de travail dont l'accès est réglementé, doivent être citoyens du Canada ou des États-Unis et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par la DSIC de TPSGC.
- (d) 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 des États-Unis et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.
- (e) 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.
- (f) 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.
- (g) 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 COMSEC / INFOSEC ou CLASSIFÉS DE L'OTAN /

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

ÉTRANGERS. 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 ».

- (h) 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 ».
- (i) 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.
- (j) En outre, l'entrepreneur ou l'offrant doit respecter les dispositions de :
 - la liste de vérification des exigences relatives à la sécurité qui se trouve à l'annexe C;
 - (ii) la plus récente version du Manuel de la sécurité industrielle.
- 2. Enlever: Section 7.5 Volet de travail 2 Très Secret, de (I) à (v) ; et

Remplacer par:

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN: DOSSIER TPSGC # W6369-17-P5LA S2 Révision # 1

- (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 NATO SECRET et TRÈS SECRET, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).
- (I) 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 devant avoir accès à des renseignements ou à des biens PROTÉGÉS/CLASSIFIÉS RESTREINS, 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 TRÈS SECRET SIGINT, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).
- (n) 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 NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléquée par l'OTAN.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME
W6369-17P5LA	004ips W6369-17P5LA	

- (o) L'entrepreneur ou l'offrant NE DOIT PAS emporter de renseignements ou de biens PROTÉGÉS/CLASSIFIÉS hors des établissements de travail visés; et l'entrepreneur ou l'offrant doit s'assurer que son personnel est au courant de cette restriction et qu'il l'a respecte.
- (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) En outre, l'entrepreneur ou l'offrant doit respecter les dispositions de :
 - la liste de vérification des exigences relatives à la sécurité qui se trouve à l'annexe C:
 - (iv) la plus récente version du Manuel de la sécurité industrielle.
- 3. Enlever: Le document entier en l'annexe C Liste de vérification des exigences relatives à la sécurité Volet de Travail 1 Secret et Volet de travail 2 Très Secret; et

Remplacer par : Le document ci-après en format PDF.

4. Enlever: Le document entier en 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; et

Remplacer par : Le document ci-après en format PDF.

5. Enlever: Le document entier en 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; et

Remplacer par : Le document ci-après en format PDF.

6. Enlever: Le document entier en Annexe A - Énoncé des travaux : Volet de Travail 1 - Secret; et

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – Nº de réf. De client	File No. – Nº du dossier	CCC No./ N° CCC – FMS No/ N° VME
W6369-17P5LA	004ips W6369-17P5LA	

Remplacer par : Le document ci-après en format PDF.

 Enlever: Le document entier en Annexe A – Énoncé des travaux : Volet de Travail 2 – Très Secret; et

Remplacer par : Le document ci-après en format PDF.

8. Enlever: La version française de « le document entier en appendice C de l'annexe A - Critères d'évaluation des ressources et tableau de réponses, Volet de travail 1 – Secret » pour harmoniser avec la version anglaise; et

Remplacer par : Le document ci-après en format PDF.

9. Enlever: La version française de « Le document entier en appendice C de l'annexe A - Critères d'évaluation des ressources et tableau de réponses, Volet de travail 2 – Très Secret » pour harmoniser avec la version anglaise; et

Remplacer par : Le document ci-après en format PDF.

10. Enlever: La version française de « Le document entier en pièce jointe 4.1: Critères d'évaluation des soumissions, Volet de travail 1 – Secret » pour harmoniser avec la version anglaise; et

Remplacer par : Le document ci-après en format PDF.

11. Enlever: La version française de « Le document entier en pièce jointe 4.1: Critères d'évaluation des soumissions, Volet de travail 2 – Très Secret » pour harmoniser avec la version anglaise; et

Remplacer par : Le document ci-après en format PDF.

QUESTIONS et RÉPONSES:

Question 35:

La section 7.5, Volet de travail 7.5 – Secret, (a) à (k), qui sont les termes du contrat qui s'appliqueront à la phase d'autorisation des tâches, et qui fût récemment amendée par l'amendement #2, indique que les exigences de sécurité pour les fournisseurs canadiens sont :

- (c) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTEGES/CLASSIFIÉS NON RESTREINTS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ en vigueur, SECRET et/ou NATO SECRET, tel que requis, délivrée ou approuvée par la DSIC de TPSGC.
- (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 résidents permanents du Canada ou citoyens d'un pays membre de l'OTAN** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **NATO SECRET**, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

Cette clause suppose que le client a la capacité et/ou la discrétion de choisir le niveau approprié de sécurité à la phase d'autorisation des tâches.

La réponse fournie à l'amendement #5, Question #33 (a) fournie ci-après, contredit ce qui est présentement indiqué aux termes et conditions du contrat, section 7.5 pour le volet de travail 1 :

a) Ceci indique seulement que le MDN aura des besoins pour des ressources de différents niveaux lesquels seront définis par voie d' 'autorisations de tâches' en attente de l'information de sécurité (Protégé, Secret, ou NATO Secret)?

Réponse 33-1 : La Couronne confirme que toutes les ressources proposées pour les exigences du volet de travail 1 à la date de fermeture des soumissions devront avoir les autorisations de sécurité SECRET et NATO SECRET avant l'octroi du contrat. La Couronne confirme aussi que toutes les ressources proposées pour les exigences du volet de travail 1 à la phase d'autorisation des tâches doivent avoir les autorisations de sécurité SECRET et NATO SECRET.

Considérant les informations fournies dans ces amendements, est-ce que la Couronne peut confirmer :

- i. Est-ce que la section 7.5 pour le volet de travail 1 modifiée par l'amendement 2 est correcte, ou est-elle substituée par la réponse à la question 33 fournie par l'amendement 5, et devrait être modifié conséquemment?
 - Réponse 35-1: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.
- ii. Est-ce que le client a la possibilité, à la phase d'autorisation des tâches, de déterminer le niveau sécurité exigé pour chacune des tâches émises, ou si toutes les ressources devront avoir l'autorisation de sécurité SECRET et NATO SECRET indépendamment des exigences, c-à-d des travaux non-OTAN?
 - Réponse 35-2 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.

S'il n'est pas de la discrétion du client et que le contrat exige les deux niveaux de sécurité, nous pensons qu'il n'est pas dans le meilleur intérêt de la Couronne, puisque notre expérience démontre que les temps de traitement pour obtenir NATO SECRET atteignent jusqu'à 210 jours ouvrables et plus dans les cas de dossiers complexes où des informations additionnelles sont requises par CISSD. Comme tel, lorsque le client débute l'octroi d'autorisations de tâches, ou le remplacement de ressources, il sera restreint à un

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

bassin limité de ressources qui pourront rencontrer cette très inhabituelle exigence. Encore une fois, nous demandons que la Couronne de reconsidère cette exigence et honore le texte tel que décrit aux termes du contrat en section 7.5?

- iii. Présentement, il n'y a pas d'indication dans l'énoncé de travail que toutes les ressources devront accéder à de l'information PROTEGES/CLASSIFIÉS NON RESTREINTS; CLASSIFIÉS RESTREINTS; et CLASSIFIÉS OTAN. Comme tel, est-ce que la Couronne peut fournir de plus amples justifications à l'effet d'avoir des autorisations de sécurité SECRET et NATO SECRET pour toutes les ressources de façon à octroyer le contrat?
 - Réponse 35-3 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.
- iv. Est-ce que toutes les ressources actuelles ont l'exigence d'avoir les autorisations SECRET et NATO SECRET. Sinon, qu'est-ce qui a changé dans la version actuelle des exigences pour justifier ce besoin?
 - Réponse 35-4 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l' 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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.

Question 36:

À la section 7.5, volet de travail 2, Très Secret, les items (i) à (v), qui sont les termes contractuels qui s'appliquent à la phase d'autorisation des tâches, et tel que fourni dans la DDP originale, indiquent que les exigences de sécurité pour les fournisseurs canadiens sont :

- (o) Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens CLASSIFIÉS RESTREINS, ou à des établissements de travail dont l'accès est réglementé, doivent être citoyens du Canada ou des États Unis *et* doivent TOUS détenir une cote de sécurité du personnel valable au niveau **TRÈS SECRET** <u>ou</u> **TRÈS SECRET** SIGINT tel que requis, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).
- (p) 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 résidents permanents du Canada ou citoyens d'un pays**

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – Nº de réf. De client	File No. – Nº du dossier	CCC No./ N° CCC – FMS No/ N° VME
W6369-17P5LA	004ips W6369-17P5LA	

membre de l'OTAN et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

Cette clause implique que le client a la capacité discrétionnaire de choisir l'autorisation de sécurité appropriée de la ressource à la phase d'autorisation de tâches.

La réponse fournie dans l'amendement 5, question 33 (a), contredit ce qui est actuellement indiqué à la section 7.5 des termes et conditions du contrat pour le volet de travail 1 :

a) Ceci indique seulement que le MDN aura des besoins pour des ressources de différents niveaux lesquels seront définis par voie d' 'autorisations de tâches' en attente de l'information de sécurité (Protégé, Secret, ou NATO Secret)?

NOTE : La Couronne assume que le demandeur se réfère plutôt au volet de travail 2 dans le deux précédents paragraphes.

Réponse 33-4: La Couronne confirme que toutes les ressources proposées pour les exigences du volet de travail 2 à la date de fermeture des soumissions devront avoir les autorisations de sécurité NATO Secret, et Top (Très) Secret, et Top (Très) Secret SIGINT avant l'octroi du contrat. La Couronne confirme aussi que toutes les ressources proposées pour les exigences du volet de travail 2 à la phase d'autorisation des tâches doivent avoir les autorisations de sécurité NATO Secret, et Top (Très) Secret, et Top (Très) Secret SIGINT.

Sur la base des informations fournies dans ces amendements, est-ce que la Couronne peut confirmer :

i. Est-ce que la section 7.5 pour le volet de travail 2, telle que stipulée dans la DDP est correcte, ou est-elle substituée par la réponse à la question 33 fournie par l'amendement 5, et devrait être modifié conséquemment?

Réponse 36-1 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

ii. Est-ce que le client a la possibilité, à la phase d'autorisation des tâches, de déterminer le niveau sécurité exigé pour chacune des tâches émises, ou si toutes les ressources devront avoir l'autorisation de sécurité TOP SECRET SIGINT, TOP SECRET et NATO SECRET indépendamment des exigences, c-à-d des travaux non-OTAN

Réponse 36-2: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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. La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

S'il n'est pas de la discrétion du client et que le contrat exige les trois niveaux de sécurité, nous pensons qu'il n'est pas dans le meilleur intérêt de la Couronne, puisque notre expérience démontre que les temps de traitement pour obtenir NATO SECRET et TS SIGINT atteignent jusqu'à 210 jours ouvrables et plus dans les cas de dossiers complexes où des informations additionnelles sont requises par CISSD. Comme tel, lorsque le client débute l'octroi d'autorisations de tâches, ou le remplacement de ressources, il sera restreint à un bassin limité de ressources qui pourront rencontrer cette très inhabituelle exigence. Encore une fois, nous demandons que la Couronne de reconsidère cette exigence et honore le texte tel que décrit aux termes du contrat en section 7.5?

iii. Présentement, il n'y a pas d'indication dans l'énoncé de travail que toutes les ressources devront accéder à de l'information PROTÉGÉS; CLASSIFIÉS RESTREINTS; et CLASSIFIÉS OTAN. Comme tel, est-ce que la Couronne peut fournir de plus amples justifications à l'effet d'avoir des autorisations de sécurité NATO SECRET, TOP SECRET et TOP SECRET SIGINT pour toutes les ressources de façon à octroyer le contrat?

Réponse 36-3 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

- iv. Est-ce toutes les ressources actuelles ont l'exigence d'avoir les autorisations NATO SECRET, Top Secret et Top Secret SIGINT. Sinon, qu'est-ce qui a changé dans la version actuelle des exigences pour justifier ce besoin?
 - a. Réponse 36-4 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l' 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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Question 37:

Pour obtenir l'autorisation de sécurité Très Secret SIGINT pour une ressource via le Portail de DSIC (CISSD), les fournisseurs sont confrontés aux instructions suivantes :

"*Justification for request (maximum 240 characters)

Warning: You have selected a personnel security clearance at the Top Secret level with SIGINT (Signals

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

Intelligence) access. A request at this level <u>must be substantiated by a specific contractual</u> requirement."

Cet avertissement ne permet pas aux fournisseurs d'utiliser la DDP et la perspective d'un potentiel contrat en tant que justification, et conséquemment, les fournisseurs ne peuvent traiter une autorisation de sécurité de niveau Très Secret SIGINT qui n'est pas justifiée par une exigence contractuelle spécifique. En maintenant les exigences de sécurité actuelles tel que stipulé à l'amendement #5, et selon les politiques du DSIC (CISSD), ceci donne aux titulaires actuels un avantage injuste. Dans le but d'assurer un marché juste et équitable et pour donner à la Couronne plus d'options et une meilleure valeur, nous demandons respectueusement d'enlever l'exigence extrêmement restrictive d'avoir toutes les autorisations de sécurité au niveau NATO SECRET, Top Secret and Top Secret SIGINT pour toutes les ressources (pour le volet de travail 2) ?

Réponse 37 : Veuillez consulter la mise-à-iour de la section 7.5 pour le volet de travail 2. la mise-à-iour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-àjour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT. Selon la section 6.1(b) de la demande de propositions: 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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires. DSIC (CISD) a confirmé qu'une autorisation de sécurité TRÈS SECRET SIGINT peut être demandée avant l'octroi d'un contrat. Un numéro valide d'appel d'offre peut être fourni à DSIC (CISD) en quise de substitut à un numéro de contrat lors d'une demande d'autorisation TRÈS SECRET SIGINT pour une ressource.

Question 38:

Selon l'amendement 5, toutes les ressources doivent posséder les autorisation de sécurité SECRET <u>et</u> NATO SECRET pour le volet de sécurité 1, et NATO SECRET, Top Secret <u>et</u> Top Secret SIGINT pour le volet de travail 2 à la date de l'octroi des contrats. Ceci est une exigence extrêmement restrictive qu'un nombre minimal de ressources pourront rencontrer et qui aura pour conséquence de limiter sérieusement le nombre de réponses de soumissionnaires pour cette sollicitation.

De plus, si un fournisseur démarrerait une demande d'autorisation de sécurité à n'importe quel niveau, pour n'importe quel candidat, avant la soumission de sa proposition, il est probable qu'il n'obtiendrait pas les autorisations nécessaires avant l'octroi des contrats, puisque notre expérience montre que les temps de traitement pour l'obtention de NATO Secret et TS SIGINT sont jusqu'à 210 jours ouvrables et plus dans les cas complexes où des informations supplémentaires sont exigées par CISSD.

Est-ce que la Couronne peut répondre aux suivantes :

Si un fournisseur soumet une proposition et est sélectionné, mais que durant le processus d'octroi des contrats, des ressources ont seulement les autorisations de sécurité pour rencontrer les exigences de la soumission, mais pas toutes les exigences du SRCL (les autorisations additionnelles étant en attente), alors, qu'arrivera t-il?

Réponse 38-1: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – Nº du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET. Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Est-ce que le fournisseur perdra l'octroi du contrat?

Réponse 38-2 :

Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l' 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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET. Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des

Solicitation No. – N° de l'invitation W6369-17P5LA/A	Amd. No – N° de la modif. 007	Buyer ID – Id de l'acheteur 004ips
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME
W6369-17P5LA	004ips W6369-17P5LA	

propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Attendu cette exigence extrêmement restrictive, est-ce que la Couronne peut identifier pour le volet de travail 1 :

Quel est le % d'autorisations de tâches qui nécessitent accès à de l'information NATO Secret?

Réponse 38-3 : 100%

Pour le volet de travail 2,

Quel est le % d'autorisations de tâches qui nécessitent accès à de l'information NATO Secret?

Réponse 38-4: 100%

Quel est le % d'autorisations de tâches qui nécessitent accès à de l'information Top Secret SIGINT?

Réponse 38-5: 100%

Est-ce que les ressources ne rencontrant les exigences de sécurité énoncés dans le SRCL pourront commencer à travailler pour des tâches spécifiques au niveau Secret et/ou Très Secret, tout en attendant que les autorisations de sécurité additionnelles soient traitées?

Réponse 38-6:

Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.

Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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. La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – N° du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

Question 39:

Référence 1A: Pièce jointe 4.1 : Critères d'évaluation des soumissions : Volet de Travail 2 – Très Secret, C.7 Spécialiste en conception de sécurité des TI – Niveau 3, Critère coté C5

Pour obtenir le maximum de points, les ressources proposées doivent avoir quatre certifications.

Référence 1B : Nous avons consulté ANNEXE A – ÉNONCÉ DES TRAVAUX W6369-17-P5LA - Volet 2, section 7.3 : C.7 – Spécialiste en conception de la sécurité des TI, niveau 3, Et nous avons noté que les tâches pour ce rôle une compréhension de la gestion des incidents.

Question 1 : La formation SANS GIAC Certified Incident Handler (GCIH) démontre une expertise dans la gestion des incidents, étant associé ainsi aux compétences exigées dans l'énoncé de travail. SVP, veuillez confirmer que le Canada acceptera la certification GCIH comme l'un des quatre points de ce critère.

Réponse 39: Après avoir considéré la demande, la Couronne à décidé de ne pas modifier les critères.

Question 40: Relativement à l' Annexe A Énoncé des travaux : Volet de Travail 1 – Secret, et à l' Annexe A Énoncé des travaux : Volet de Travail 2 – Très Secret; sous-section 6. Période de transition, 6.1.1.1 déclare : 'L'entrepreneur doit fournir un plan de transition détaillé dans les trois (3) semaines suivant l'attribution du contrat,' Subséquemment à cet énoncé, à la section 6.2, Plan de transition : Le soumissionnaire doit décrire l'approche, la méthodologie et la gestion des évaluations des risques qu'il prévoit adopter pour répondre aux exigences de la période de transition.... Il est très peu fréquent d'avoir un critère évaluation de soumission spécifié dans un énoncé de travail. Le soumissionnaire soupçonne un défaut de terminologie (soumissionnaire VS entrepreneur). Veuillez confirmer qu'à la section 6.2, la référence au 'soumissionnaire' devrait être lue en tant qu' 'entrepreneur'.

Réponse 40 : Veuillez consulter la mise-à-jour de l'Annexe A – Énoncé de travail- Volet de travail 1, et Volet de travail 2 en section 6.2 : La référence au 'soumissionnaire' est remplacé par 'Entrepreneur'.

Question 41:

Q 41-1) Pouvez-vous confirmer que pour le volet de travail 1 de la demande de propositions, les ressources proposées peuvent avoir des autorisations de sécurité de niveau Secret **et/ou** NATO Secret **et/ou** Fiabilité; cependant, avant que les contrats soient octroyés aux soumissionnaires, ces mêmes ressources doivent avoir les deux autorisations Secret **et** NATO Secret?

Réponse 41-1: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET.

Q41-2) De façon similaire, **pouvez-vous confirmer** que pour le volet de travail 2 de la demande de propositions, les ressources proposées doivent avoir les autorisations de sécurité NATO Secret

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client W6369-17P5LA	File No. – Nº du dossier 004ips W6369-17P5LA	CCC No./ N° CCC – FMS No/ N° VME

et/ou Très Secret **et/ou** Très Secret SIGINT; cependant, avant l'octro des contrats, les mêmes ressources doivent avoir toutes les autorisations NATO Secret <u>et</u> Très Secret <u>et</u> Très Secret SIGINT?

Réponse 41-2: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Q41-3) Si notre compréhension en Q42-1 est correcte, en sachant le délai requis pour obtenir ces autorisations en considérant les arrérages à DSIC (CISD) et qu'en réalité, les soumissionnaires ont peu de contrôle sur le processus d'octroi des autorisations de sécurité, nous demandons que, en autant que les ressources ont une autorisation de sécurité Secret pour le volet de travail 1, qu'une demande à DSIC fût initié à la date d'octroi des contrats et montre au minimum le statut 'en cours', que ceci soit acceptable? Pouvez-vous confirmer?

Réponse 41-3: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 1, la miseà-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 1). et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 1 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens ou américains, et doivent chacune détenir une autorisation de sécurité NATO SECRET. Selon la section 6.1(b) de la demande de propositions : 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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Q 41-4: Si notre compréhension de la question 42-2 est correcte, en sachant le délai requis pour obtenir ces autorisations en considérant les arrérages à DSIC (CISD) et qu'en réalité, les soumissionnaires ont peu de contrôle sur le processus d'octroi des autorisations de sécurité, nous demandons que, <u>en autant que les ressources ont une autorisation de sécurité Très Secret pour le volet de travail 2, qu'une demande à DSIC fût initié à la date d'octroi des contrats et montre au minimum le statut 'en cours', que ceci soit acceptable? Pouvez-vous confirmer?</u>

Réponse 41-4 : Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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 . La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LA/A	007	004ips
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME
W6369-17P5LA	004ips W6369-17P5LA	

chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires.

Q 41-5) Relativement à l'exigence pour l'autorisation Très Secret SIGINT pour les ressources proposées du volet de travail 2, notre expérience avec DSIC est que les autorisations Très Secret SIGINT ne peuvent être demandées que lorsqu'un contrat est octroyé, et qu'il inclue des exigences pour ce niveau de sécurité; un numéro de contrat est requis à l'intérieur de la demande d'autorisation pour un individu à ce niveau. Ceci étant le cas, nous demandons que l'autorisation Très Secret SIGINT ne soit requise qu'à la phase d'octroi des tâches. Pouvez-vous confirmer?

Réponse 41-5: Veuillez consulter la mise-à-jour de la section 7.5 pour le volet de travail 2, la mise-à-jour de l'Annexe C Liste de vérification des exigences relatives à la sécurité (Volet de travail 2), et la mise-à-jour de l'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. La Couronne confirme que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences doivent, à la date de clôture des propositions, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT avant l'octroi des contrats. La Couronne confirme aussi que toutes les ressources du volet de travail 2 présentées pour répondre aux catégories d'exigences, doivent à la phase d'octroi de tâches, être citoyens canadiens, et doivent chacune détenir les deux autorisations de sécurité NATO SECRET et TRÈS SECRET-SIGINT.

Selon la section 6.1(b) de la demande de propositions : '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.' . Veuillez aussi noter que l'exigence inclue le processus Foreign Ownership, Control and Influence (FOCI), donc en conséquence, il y aura parallèlement assez de temps pour obtenir les autorisations de sécurité nécessaires pour tous les soumissionnaires. DSIC (CISD) a confirmé qu'une autorisation de sécurité TRÈS SECRET SIGINT peut être demandée avant l'octroi d'un contrat. Un numéro valide d'appel d'offre peut être fourni à DSIC (CISD) en guise de substitut à un numéro de contrat lors d'une demande d'autorisation TRÈS SECRET SIGINT pour une ressource.

TOUTES LES AUTRES MODALITÉS DEMEURENT INCHANGÉES.
NOTA: UNE SOUMISSIONS DÉJÀ PRÉSENTÉE PEUT ÊTRE MODIFIÉE AVANT LA
DATE DE CLÔTURE.
LA CORRESPONDANCE CONCERNANT LA MODIFICATIONS DOIT INDIQUER LE
NUMÉRO DE LA DEMANDE DE SOUMISSIONS ET LA DATE DE CLÔTURE DES
SOUMISSIONS; ELLE SOIT ÊTRE ADRESSÉE À:
RÉCEPTION DES SOUMISSIONS
SERVICES PUBLICS ET APPROVISIONNEMENT CANADA
PLACE DU PORTAGE, PHASE III
HALL PRINCIPAL, SALLE 0A1
11, RUE LAURIER
GATINEAU (QUÉBEC) K1A 0S5

ANNEXE A – ÉNONCÉ DES TRAVAUX W6369-17-P5LA – Volet 1

1. CONTEXTE

- 1.1. La Direction de l'ingénierie et de l'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 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'architecture 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. L'ingénierie relative à la cybersécurité et les services d'architecture (DIIGI 3) se composent de six services essentiels :
 - 1.2.1. Orientation sur la 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 assureront 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.

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 être prise en charge, ce qui crée des besoins pour des connaissances, des compétences et de l'expérience variées.
- 3.2. Les ressources travailleront principalement avec le personnel de la DIIGI du MDN. Toutefois, dans certaines occasions, 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 APPLICABLES

- 4.1. Au besoin, le responsable (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 de l'horaire normal de travail doit avoir été approuvé au préalable par le RT par écrit. 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 sera requise à la suite de l'attribution du contrat au nouvel entrepreneur retenu pour ce besoin. Cette période de transition laissera au nouvel entrepreneur le temps de préparer ses ressources, d'assumer ses responsabilités et d'atteindre un état de stabilité. Elle donnera aussi à l'entrepreneur titulaire le temps de terminer ses activités en cours. L'entrepreneur titulaire transfère au nouvel entrepreneur les responsabilités des activités en cours et des activités prévues à la fin de la période de transition.
 - 6.1.1. La période de transition débutera à la date d'attribution du contrat et se terminera environ deux (2) ans après l'attribution du contrat. Dans le but de garantir la transition des services actuels de soutien d'ingénierie et d'architecture de gestion de l'information et technologie de l'information (GI-TI) à la pleine mise en œuvre des services décrit dans le présent énoncé des travaux, et ce, sans interruption du soutien ou perturbation des processus et activités du ministère de la Défense nationale (MDN), l'entrepreneur doit prendre les mesures 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, afin d'assurer une transition efficace pour toutes les ressources et activités et de permettre une configuration ordonnée et rapide afin de répondre à toutes les exigences du MDN mentionnées dans l'énoncé des travaux. Le plan de travail sera élaboré en collaboration avec le MDN et approuvé par l'autorité technique.
- 6.1.1.2. Conformément au plan de transition, la transition se termine par le transfert des responsabilités du titulaire à l'entrepreneur.
- 6.2. <u>Plan de transition</u>: L'entrepreneur doit décrire l'approche, la méthodologie et la gestion des évaluations des risques qu'il prévoit adopter pour répondre aux exigences de la période de transition.
 - 6.2.1. La description doit inclure à tout le moins les composantes suivantes :
 - a. la portée, les buts et l'objectif de la transition;
 - b. les activités à réaliser pendant la transition;
 - c. les ressources et le niveau d'efforts requis pour réaliser chaque activité;
 - d. les rôles et les responsabilités du personnel clé;
 - e. la gestion des évaluations des risques;
 - les échéanciers proposés pour toutes les activités et sous-activités et les jalons connexes.

7. TÂCHES ET PRODUITS LIVRABLES

7.1. P.1 - Conseiller en gestion du changement, niveau 3

Le consultant en gestion du changement de niveau 3 doit :

- 7.1.1. Créer des échéanciers et des plans de travail;
- 7.1.2. Analyser et élaborer des « facteurs critiques du succès » dans les opérations;
- 7.1.3. Examiner, analyser et élaborer la conception des exigences liées à l'architecture, la conception des processus, la schématisation de processus et la formation;
- 7.1.4. Élaborer des documents de gestion de projet conformément aux directives du guide Project Management Body of Knowledge (PMBOK);
- 7.1.5. Offrir du soutien à la gestion des documents à l'aide de Microsoft SharePoint;
- 7.1.6. Définir les stratégies et les processus opérationnels qui favoriseront les activités de transformation et de gestion du changement, et ce, en collaboration avec d'autres employés fonctionnels du MDN et de la DIIGI;
- 7.1.7. Participer à l'analyse des répercussions du changement et des activités de gestion du changement et l'examiner;
- 7.1.8. Mettre en œuvre le remaniement et le réaménagement organisationnel en collaboration avec d'autres employés fonctionnels du MDN et de la DIIGI;
- 7.1.9. Concevoir du matériel de formation avec d'autres intervenants;

- 7.1.10. Créer des exposés et les présenter à divers intervenants, ainsi qu'animer des réunions et des discussions;
- 7.1.11. Participer aux réunions et aux groupes de travail, à la demande du RT;
- 7.1.12. Réaliser des vérifications des processus de gestion de la configuration et du changement;
- 7.1.13. Transmettre au RT par courriel chaque semaine des comptes rendus concernant toute demande de changements en attente ou en suspens;
- 7.1.14. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.2. P.9 – Gestionnaire de projet, niveau 3

Le gestionnaire de projet de niveau 3 doit :

- 7.2.1. Créer des échéanciers et des plans de travail;
- 7.2.2. Gérer plusieurs gestionnaires de projet, chacun d'eux étant responsable d'un élément du projet et de l'équipe de projet connexe;
- 7.2.3. Élaborer des documents de gestion de projet conformément aux directives du guide Project Management Body of Knowledge (PMBOK);
- 7.2.4. Créer, appuyer, mettre à jour et suivre des projets à l'aide de Microsoft Project;
- 7.2.5. Fournir du soutien à la gestion des documents;
- 7.2.6. Gérer l'élaboration et la mise en œuvre et le début des projets, en veillant à ce que les ressources soient disponibles et que les projets soient développés et totalement fonctionnels selon les contraintes de délai, de coût et de rendement établies à l'avance;
- 7.2.7. Planifier, évaluer, suivre et surveiller les activités d'une équipe de projet dans les délais et les paramètres financiers prévus, puis prodiguer des conseils;
- 7.2.8. Formuler des énoncés de problèmes, et établir des procédures servant à élaborer et à mettre en œuvre des éléments de projets, nouveaux ou modifiés dans le but de résoudre ces problèmes;
- 7.2.9. Définir et documenter les jalons des projets en plus d'établir les exigences financières, les rôles et les responsabilités ainsi que le mandat des équipes des projets;
- 7.2.10. Faire continuellement état des progrès réalisés dans le cadre des projets;
- 7.2.11. S'occuper de la planification et de la gestion des affaires financières;
- 7.2.12. Superviser et coordonner les ressources en cas de nouvelles exigences;
- 7.2.13. Examiner les exigences opérationnelles, ce qui comprend la gestion de contrat et le suivi de l'approvisionnement;
- 7.2.14. Diriger les réunions et les groupes de travail, à la demande du RT;
- 7.2.15. Rédiger des documents d'information et les transmettre aux intervenants et aux autres gestionnaires de projet;

- 7.2.16. Créer des exposés et les présenter à divers intervenants, ainsi qu'animer des réunions et des discussions;
- 7.2.17. Élaborer des plans, des graphiques, des tableaux et des diagrammes en vue d'aider à analyser ou à présenter des problèmes ainsi que travailler avec divers outils de gestion de projets.
- 7.2.18. Concevoir du matériel de formation avec d'autres intervenants;
- 7.2.19. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.3. C.5 – Spécialistes de l'ICP, niveaux 2 et 3

Les spécialistes de l'ICP de niveaux 2 et 3 doivent :

- 7.3.1. Créer des échéanciers et des plans de travail;
- 7.3.2. Élaborer des politiques, des normes, des lignes directrices et des procédures relatives à l'ICP:
- 7.3.3. Examiner, analyser et évaluer les politiques, les normes, les lignes directrices et les procédures en vigueur en matière d'ICP, et prodiguer des conseils quant à leur pertinence et à leur efficacité;
- 7.3.4. Examiner, analyser, évaluer les éléments suivants et prodiguer des conseils à leur égard :
 - 7.3.4.1. l'architecture de l'ICP;
 - 7.3.4.2. les certificats et signatures numériques;
 - 7.3.4.3. les produits d'ICP;
 - 7.3.4.4. les produits ou solutions reposant sur les clés publiques;
 - 7.3.4.5. les normes d'annuaire, comme X.500;
 - 7.3.4.6. les normes de certificat, comme X.509;
 - 7.3.4.7. protocoles de sécurité Internet (TSL, S-MIME, IPSec, SSH, etc.);
 - 7.3.4.8. la conception, le développement et les services d'autorité de certification (AC);
- 7.3.5. 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;
- 7.3.6. 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;
- 7.3.7. Architecturer, concevoir, élaborer, mettre à l'essai, consigner et mettre en œuvre les solutions d'ICP, entre autres : l'autorité de certification Entrust, l'autorité de

- certification Microsoft, les modules de sécurité matériels, les solutions de gestion des cartes, les cartes à puce, le logiciel client Entrust, les logiciels de carte à puce et les applications conformes à l'ICP;
- 7.3.8. Fournir de l'orientation aux équipes de soutien technique sur l'ICP et les applications connexes et s'assurer que les nouvelles applications n'interfèrent pas avec l'infrastructure actuelle;
- 7.3.9. Formuler des commentaires sur les aspects des systèmes applicatifs en cours de développement qui concernent les ICP;
- 7.3.10. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.3.11. Élaborer et fournir une trousse de matériel de formation pertinente à l'ICP;
- 7.3.12. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.4. C.6 – Ingénieur en sécurité des TI, niveaux 1 à 3

Les ingénieurs en sécurité des TI de niveaux 1 à 3 doivent :

- 7.4.1. Créer des échéanciers et des plans de travail;
- 7.4.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.4.2.1. les normes d'annuaire comme X.500 et LDAP;
 - 7.4.2.2. les systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.4.2.3. les protocoles réseau comme HTTP, FTP et Telnet;
 - 7.4.2.4. les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, TSL et SSH;
 - 7.4.2.5. les protocoles de sécurité des TI pour toutes les couches de l'OSI (Interconnexion des systèmes ouverts) et toutes les piles TCP/IP (Transmission Control Protocol/Internet Protocol);
 - 7.4.2.6. les protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau);
 - 7.4.2.7. les routeurs, les multiplexeurs et les commutateurs réseau;
 - 7.4.2.8. les techniques de renforcement de la sécurité des applications, des hôtes ou du réseau, les produits et les pratiques exemplaires en matière de sécurité (p. ex., procédure d'interpréteur de commandes [shell scripting], identification des services et contrôle des accès);
 - 7.4.2.9. les systèmes de détection/prévention des intrusions, la défense contre les codes malveillants, l'intégrité des fichiers, la gestion de la sécurité d'entreprise et les pare-feu;
 - 7.4.2.10. la technologie sans fil;

- 7.4.2.11. les algorithmes cryptographiques.
- 7.4.3. Élaborer et mettre en œuvre des applications et des infrastructures de sécurité des applications dans divers domaines, notamment les suivants :
 - 7.4.3.1. systèmes de prévention des intrusions au niveau de l'hôte;
 - 7.4.3.2. technologies de sécurité de réseautage sans fil;
 - 7.4.3.3. systèmes de détection des intrusions;
 - 7.4.3.4. systèmes de prévention des intrusions réseau;
 - 7.4.3.5. gestion de l'information et des incidents de sécurité;
 - 7.4.3.6. saisie intégrale des paquets;
 - 7.4.3.7. contrôle de l'accès réseau;
 - 7.4.3.8. gestion de l'identité, des justificatifs d'identité et de l'accès;
 - 7.4.3.9. protection des points terminaux.
- 7.4.4. Déceler et analyser les menaces techniques pesant sur les réseaux et les vulnérabilités de ces derniers;
- 7.4.5. Examiner et analyser les éléments suivants, puis présenter des rapports à leur égard :
 - 7.4.5.1. les outils et les techniques de sécurité des TI;
 - 7.4.5.2. les données de sécurité et la présentation d'avis et de rapports;
 - 7.4.5.3. les analyses statistiques de la sécurité des TI;
 - 7.4.5.4. la gestion de la configuration de la sécurité des TI.
- 7.4.6. Rédiger des plans d'analyse et de mise en œuvre des options de solutions de sécurité des TI;
- 7.4.7. 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;
- 7.4.8. Fournir un soutien pour la vérification et la validation par un tiers dans le cadre des projets de sécurité des TI, notamment :
 - 7.4.8.1. les vérifications de sécurité des TI, y compris les rapports, présentations et autres documents applicables;
 - 7.4.8.2. l'examen des plans d'urgence, des plans de continuité des activités et des plans de reprise après sinistre;
 - 7.4.8.3. la conception ou l'élaboration de protocoles de sécurité des TI;
 - 7.4.8.4. l'élaboration et la réalisation de tests et d'exercices;
 - 7.4.8.5. la supervision de projets.
- 7.4.9. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:

- 7.4.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;
- 7.4.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.5. C.7 - Spécialiste en conception de la sécurité des TI, niveaux 2 et 3

Les spécialistes en conception de sécurité des TI de niveaux 2 et 3 doivent :

- 7.5.1. Créer des échéanciers et des plans de travail;
 - 7.5.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.5.2.1. les normes d'annuaire comme X.500 et LDAP;
 - 7.5.2.2. les systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.5.2.3. les protocoles réseau comme HTTP, FTP et Telnet;
 - 7.5.2.4. les routeurs, les multiplexeurs et les commutateurs réseau;
 - 7.5.2.5. les protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau);
 - 7.5.2.6. les architectures sécurisées des TI, normes, et protocoles de communications et de sécurité comme IPSec, TSL, SSH, S-MIME, HTTPS;
 - 7.5.2.7. les protocoles de sécurité des TI pour toutes les couches de l'OSI (interconnexion des systèmes ouverts) et toutes les piles TCP/IP;
 - 7.5.2.8. l'importance et les implications des tendances du marché et des technologies afin de les appliquer dans le cadre des feuilles de route pour les architectures et de la conception des solutions (p. ex., la sécurité des services Web, la gestion des incidents, la gestion de l'identité);
 - 7.5.2.9. les pratiques exemplaires et les normes en matière de zonage réseau et des principes de défense en profondeur.
- 7.5.3. Analyser les outils et les techniques de sécurité des TI;
- 7.5.4. Analyser les données de sécurité et présenter des avis et des rapports;
- 7.5.5. 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;
- 7.5.6. Rédiger des rapports techniques : analyse des besoins, analyse des possibilités, documents d'architecture technique, modélisation mathématique des risques, etc.;
- 7.5.7. Assurer la conception d'architectures de sécurité et le soutien technique;
- 7.5.8. Effectuer des analyses statistiques de la sécurité des TI;

- 7.5.9. Réaliser des études liées à la classification ou à la désignation de sécurité des données:
- 7.5.10. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.5.11. Créer des alertes et des avis de sécurité des TI sur mesure provenant de sources publiques et privées;
- 7.5.12. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;
- 7.5.13. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

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

Les analystes de la sécurité des réseaux de niveaux 2 et 3 doivent :

- 7.6.1. Créer des échéanciers et des plans de travail;
- 7.6.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.6.2.1. les normes d'annuaire comme X.500 et LDAP;
 - 7.6.2.2. les systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.6.2.3. les protocoles réseau comme HTTP, FTP et Telnet;
 - 7.6.2.4. les protocoles de sécurité Internet (TSL, HTTPS, S-MIME, IPSec, SSH),
 - 7.6.2.5. les protocoles comme TCP/IP, UDP, DNS, LDAP et autres protocoles applicables;
 - 7.6.2.6. les routeurs, les multiplexeurs et les commutateurs réseau;
 - 7.6.2.7. les techniques de renforcement des réseaux, notamment procédure d'interpréteur de commandes [shell scripting], identification des services et contrôle des accès);
 - 7.6.2.8. les algorithmes cryptographiques approuvés par le gouvernement;
 - 7.6.2.9. les systèmes de détection et de prévention des intrusions et pare-feu;
 - 7.6.2.10. les mesures de protection techniques des TI; et
 - 7.6.2.11. la technologie sans fil;
- 7.6.3. Élaborer et mettre en œuvre des applications et des infrastructures de sécurité des applications dans divers domaines, notamment les suivants :
 - 7.6.3.1. systèmes de prévention des intrusions au niveau de l'hôte;
 - 7.6.3.2. technologies de sécurité de réseautage sans fil;
 - 7.6.3.3. systèmes de détection des intrusions;
 - 7.6.3.4. systèmes de prévention des intrusions réseau;
 - 7.6.3.5. gestion de l'information et des incidents de sécurité;
 - 7.6.3.6. saisie intégrale des paquets;

- 7.6.3.7. contrôle de l'accès réseau;
- 7.6.3.8. gestion de l'identité, des justificatifs d'identité et de l'accès;
- 7.6.3.9. protection des points terminaux.
- 7.6.4. Analyser et renforcer les outils et les techniques de sécurité des TI;
- 7.6.5. Analyser les données de sécurité et présenter des avis et des rapports;
- 7.6.6. Analyser les répercussions de la mise en œuvre de nouveaux logiciels et de modifications de configuration importantes ainsi que de la gestion des correctifs;
- 7.6.7. Élaborer des modèles de validation et des essais pour la sécurité des TI;
- 7.6.8. la conception ou l'élaboration de protocoles de sécurité des TI;
- 7.6.9. Déceler et analyser les menaces techniques pesant sur les réseaux et les vulnérabilités de ces derniers;
- 7.6.10. Créer des alertes et des avis de sécurité des TI sur mesure provenant de sources publiques et privées;
- 7.6.11. Effectuer les tâches associées à l'autorisation et à l'authentification sécurisées dans les réseaux et applications physiques et logiques;
- 7.6.12. Examiner et analyser les journaux de sécurité aux fins des événements de sécurité dans le but de concevoir des garanties et des contre-mesures;
- 7.6.13. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.6.14. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

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. Tous les rapports d'étape doivent 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. Toute recommandation visant la mise à jour des 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 effectués dans les installations du MDN, dans la RCN.

11. DÉPLACEMENTS

- 11.1. Les frais de déplacement au sein de la région 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 W6369-17-P5LA - Volet 2

1. CONTEXTE

- 1.1. La Direction de l'ingénierie et de l'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 technologie de l'information (GI-TI) pour le ministère de la Défense nationale et les Forces armées canadiennes (MDN et FAC). Elle soutient le dirigeant principal de l'information de la Défense en qualité d'ingénieur en chef et d'architecture en chef et 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 sur la sécurité technique : correspond à l'élaboration, à l'interprétation ou à la mise en œuvre des normes techniques sur la sécurité 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 clé publique (ICP) 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 et validation de la sécurité : 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 document concerne la prestation de services d'ingénierie et d'architecture de GI-TI au MDN. Les travaux exécutés dans le cadre du présent contrat assureront 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.

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 être prise en charge, ce qui crée des besoins pour des connaissances, des compétences et de l'expérience variées.
- 3.2. Les ressources travailleront principalement avec le personnel de la DIIGI du MDN. Toutefois, dans certaines occasions, 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 APPLICABLES

- 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 de l'horaire normal de travail doit avoir été approuvé au préalable par l'autorité technique par écrit. Si une 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 sera requise à la suite de l'attribution du contrat au nouvel entrepreneur retenu pour ce besoin. Cette période de transition laissera au nouvel entrepreneur le temps de préparer ses ressources, d'assumer ses responsabilités et d'atteindre un état de stabilité. Elle donnera aussi à l'entrepreneur titulaire le temps de terminer ses activités en cours. L'entrepreneur titulaire transfère au nouvel entrepreneur les responsabilités des activités en cours et des activités prévues à la fin de la période de transition.
 - 6.1.1. La période de transition débutera à la date d'attribution du contrat et se terminera environ deux (2) ans après l'attribution du contrat. Dans le but de garantir la transition des services actuels de soutien d'ingénierie et d'architecture de gestion de l'information et technologie de l'information (GI-TI) à la pleine mise en œuvre des services décrit dans le présent énoncé des travaux, et ce, sans interruption du soutien ou perturbation des processus et activités du ministère de la Défense nationale (MDN), l'entrepreneur doit prendre les mesures 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, afin d'assurer une transition efficace pour toutes les

ressources et activités et de permettre une configuration ordonnée et rapide afin de répondre à toutes les exigences du MDN mentionnées dans l'énoncé des travaux. Le plan de travail sera élaboré en collaboration avec le MDN et approuvé par l'autorité technique.

- 6.1.1.2. Conformément au plan de transition, la transition se termine par le transfert des responsabilités du titulaire à l'entrepreneur.
- 6.2. <u>Plan de transition</u>: L'entrepreneur doit décrire l'approche, la méthodologie et la gestion des évaluations des risques qu'il prévoit adopter pour répondre aux exigences de la période de transition.
 - 6.2.1. La description doit inclure à tout le moins les composantes suivantes :
 - a. la portée, les buts et l'objectif de la transition;
 - b. les activités à réaliser pendant la transition;
 - c. les ressources et le niveau d'efforts requis pour réaliser chaque activité;
 - d. les rôles et les responsabilités du personnel clé;
 - e. la gestion des évaluations des risques;
 - f. les échéanciers proposés pour toutes les activités et sous-activités et les jalons connexes.

7. TÂCHES ET PRODUITS LIVRABLES

7.1. C.5 – Spécialiste de l'ICP – Niveau 3

Les spécialistes de l'ICP de niveau 3 doivent :

- 7.1.1. Créer des échéanciers et des plans de travail:
- 7.1.2. Élaborer des politiques, des normes, des lignes directrices et des procédures relatives à l'ICP;
- 7.1.3. Examiner, analyser et évaluer les politiques, les normes, les lignes directrices et les procédures en vigueur en matière d'ICP, et prodiguer des conseils quant à leur pertinence et à leur efficacité;
- 7.1.4. Examiner, analyser, évaluer les éléments suivants et prodiguer des conseils à leur égard :
 - 7.1.4.1. architecture de l'ICP;
 - 7.1.4.2. certificats et signatures numériques;
 - 7.1.4.3. produits d'ICP;
 - 7.1.4.4. produits ou solutions reposant sur les clés publiques;
 - 7.1.4.5. normes d'annuaire, comme X.500;
 - 7.1.4.6. normes de certificat, comme X.509;
 - 7.1.4.7. protocoles de sécurité Internet (TSL, S-MIME, IPSec, SSH, etc.);
 - 7.1.4.8. conception, développement et services d'autorité de certification (AC);

- 7.1.5. 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;
- 7.1.6. 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;
- 7.1.7. Architecturer, concevoir, élaborer, mettre à l'essai, consigner et mettre en œuvre les solutions d'ICP, entre autres : l'autorité de certification Entrust, l'autorité de certification Microsoft, les modules de sécurité matériels, les solutions de gestion des cartes, les cartes à puce, le logiciel client Entrust, les logiciels de carte à puce et les applications conformes à l'ICP;
- 7.1.8. Fournir de l'orientation aux équipes de soutien technique sur l'ICP et les applications connexes et s'assurer que les nouvelles applications n'interfèrent pas avec l'infrastructure actuelle:
- 7.1.9. Formuler des commentaires écrits sur les aspects des systèmes applicatifs en cours d'élaboration qui concernent l'ICP;
- 7.1.10. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT;
- 7.1.11. Élaborer et fournir une trousse de matériel de formation pertinente à l'ICP;
- 7.1.12. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.2. C.6 – Ingénieur en sécurité des TI – Niveaux 1 à 3

Les ingénieurs en sécurité des TI de niveaux 1 à 3 doivent :

- 7.2.1. Créer des échéanciers et des plans de travail;
- 7.2.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.2.2.1. normes d'annuaire comme X.500 et LDAP;
 - 7.2.2.2. systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.2.2.3. protocoles réseau comme HTTP, FTP et Telnet;
 - 7.2.2.4. notions de base des architectures sécurisées des TI, normes et protocoles de communications et de sécurité comme IPSec, IPv6, TSL et SSH;
 - 7.2.2.5. protocoles de sécurité des TI pour toutes les couches de l'OSI (Interconnexion des systèmes ouverts) et toutes les piles TCP/IP (Transmission Control Protocol/Internet Protocol);

- 7.2.2.6. protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau);
- 7.2.2.7. routeurs, multiplexeurs et commutateurs réseau;
- 7.2.2.8. techniques de renforcement de la sécurité des applications, des hôtes ou du réseau, produits et les pratiques exemplaires en matière de sécurité (p. ex., procédure d'interpréteur de commandes [shell scripting], identification des services et contrôle des accès);
- 7.2.2.9. systèmes de détection/prévention des intrusions, défense contre les codes malveillants, intégrité des fichiers, gestion de la sécurité d'entreprise et coupefeu;
- 7.2.2.10. technologie sans fil;
- 7.2.2.11. algorithmes cryptographiques approuvés par le gouvernement;
- 7.2.3. Élaborer et mettre en œuvre des applications et des infrastructures de sécurité des applications dans divers domaines, notamment les suivants :
 - 7.2.3.1. systèmes de prévention des intrusions au niveau de l'hôte;
 - 7.2.3.2. technologies de sécurité de réseautage sans fil;
 - 7.2.3.3. systèmes de détection des intrusions;
 - 7.2.3.4. systèmes de prévention des intrusions dans un réseau;
 - 7.2.3.5. gestion de l'information et des incidents de sécurité;
 - 7.2.3.6. saisie intégrale des paquets;
 - 7.2.3.7. contrôle de l'accès au réseau;
 - 7.2.3.8. gestion de l'identité, des justificatifs d'identité et de l'accès;
 - 7.2.3.9. protection des points terminaux;
- 7.2.4. Déceler et analyser les menaces techniques pesant sur les réseaux et les vulnérabilités de ces derniers;
- 7.2.5. Examiner et analyser les éléments suivants, puis présenter des rapports à leur égard :
 - 7.2.5.1. outils et techniques de sécurité des TI;
 - 7.2.5.2. données de sécurité et présentation d'avis et de rapports;
 - 7.2.5.3. analyses statistiques de la sécurité des TI;
 - 7.2.5.4. gestion de la configuration de la sécurité des TI;
- 7.2.6. Rédiger des plans d'analyse et de mise en œuvre des options de solutions de sécurité des TI:
- 7.2.7. 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;

- 7.2.8. Fournir un soutien pour la vérification et la validation par un tiers dans le cadre des projets de sécurité des TI, notamment :
 - 7.2.8.1. les vérifications de sécurité des TI, y compris les rapports, présentations et autres documents applicables;
 - 7.2.8.2. l'examen des plans d'urgence, des plans de continuité des activités et des plans de reprise après sinistre;
 - 7.2.8.3. la conception ou élaboration de protocoles de sécurité des TI;
 - 7.2.8.4. l'élaboration et la réalisation de tests et d'exercices;
 - 7.2.8.5. la supervision de projets.
- 7.2.9. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT;
- 7.2.10. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de l'ingénierie de la sécurité des TI;
- 7.2.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.3. C.7 – Spécialiste en conception de la sécurité des TI, niveau 3

Les spécialistes en conception de sécurité des TI de niveau 3 doivent :

- 7.3.1. Créer des échéanciers et des plans de travail;
- 7.3.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.3.2.1. normes d'annuaire comme X.500 et LDAP;
 - 7.3.2.2. systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.3.2.3. protocoles réseau comme HTTP, FTP et Telnet;
 - 7.3.2.4. routeurs, multiplexeurs et commutateurs réseau;
 - 7.3.2.5. protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau):
 - 7.3.2.6. architectures sécurisées des TI, normes, et protocoles de communications et de sécurité comme IPSec, TSL, SSH, S-MIME, HTTPS;
 - 7.3.2.7. protocoles de sécurité des TI pour toutes les couches de l'OSI (interconnexion des systèmes ouverts) et toutes les piles TCP/IP;
 - 7.3.2.8. l'importance et implications des tendances du marché et des technologies afin de les appliquer dans le cadre des feuilles de route pour les architectures et de la conception des solutions (p. ex. la sécurité des services Web, la gestion des incidents, la gestion de l'identité);
 - 7.3.2.9. pratiques exemplaires et normes en matière de zonage réseau et des principes de défense en profondeur;
- 7.3.3. Analyser les outils et les techniques de sécurité des TI;

- 7.3.4. Analyser les données de sécurité et présenter des avis et des rapports;
- 7.3.5. 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;
- 7.3.6. Rédiger des rapports techniques : analyse des besoins, analyse des options, documents d'architecture technique, modélisation mathématique des risques, etc.;
- 7.3.7. Assurer la conception d'architectures de sécurité et le soutien technique;
- 7.3.8. Effectuer des analyses statistiques de la sécurité des TI;
- 7.3.9. Réaliser des études liées à la classification ou à la désignation de sécurité des données:
- 7.3.10. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.3.11. Créer des alertes et des avis de sécurité des TI sur mesure provenant de sources publiques et privées;
- 7.3.12. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à l'évaluation de la conception de la sécurité des TI;
- 7.3.13. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

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

Les analystes de la sécurité des réseaux de niveau 3 doivent :

- 7.4.1. Créer des échéanciers et des plans de travail;
- 7.4.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, entre autres :
 - 7.4.2.1. normes d'annuaire comme X.500 et LDAP;
 - 7.4.2.2. systèmes d'exploitation, comme Microsoft, Unix et Linux;
 - 7.4.2.3. protocoles réseau comme HTTP, FTP et Telnet;
 - 7.4.2.4. protocoles de sécurité Internet (TSL, HTTPS, S-MIME, IPSec, SSH);
 - 7.4.2.5. protocoles comme TCP/IP, UDP, DNS, LDAP et autres protocoles applicables;
 - 7.4.2.6. routeurs, multiplexeurs et commutateurs réseau;
 - 7.4.2.7. techniques de renforcement des réseaux, notamment procédure d'interpréteur de commandes [shell scripting], identification des services et contrôle des accès);
 - 7.4.2.8. algorithmes cryptographiques approuvés par le gouvernement;
 - 7.4.2.9. systèmes de détection et de prévention des intrusions et pare-feu;
 - 7.4.2.10. mesures de protection techniques des TI;

- 7.4.2.11. technologie sans fil.
- 7.4.3. Élaborer et mettre en œuvre des applications et des infrastructures de sécurité des applications dans divers domaines, notamment les suivants :
 - 7.4.3.1. systèmes de prévention des intrusions au niveau de l'hôte;
 - 7.4.3.2. technologies de sécurité de réseautage sans fil;
 - 7.4.3.3. systèmes de détection des intrusions;
 - 7.4.3.4. systèmes de prévention des intrusions dans un réseau;
 - 7.4.3.5. gestion de l'information et des incidents de sécurité;
 - 7.4.3.6. saisie intégrale des paquets;
 - 7.4.3.7. contrôle de l'accès au réseau;
 - 7.4.3.8. gestion de l'identité, des justificatifs d'identité et de l'accès;
 - 7.4.3.9. protection des points terminaux.
- 7.4.4. Analyser et renforcer les outils et les techniques de sécurité des TI;
- 7.4.5. Analyser les données de sécurité et présenter des avis et des rapports;
- 7.4.6. Analyser les répercussions de la mise en œuvre de nouveaux logiciels et de modifications de configuration importantes ainsi que de la gestion des correctifs;
- 7.4.7. Élaborer des modèles de validation et des essais pour la sécurité des TI;
- 7.4.8. Concevoir/élaborer des protocoles de sécurité des TI;
- 7.4.9. Déceler et analyser les menaces techniques pesant sur les réseaux et les vulnérabilités de ces derniers;
- 7.4.10. Créer des alertes et des avis de sécurité des TI sur mesure provenant de sources publiques et privées;
- 7.4.11. Effectuer les tâches associées à l'autorisation et à l'authentification sécurisées dans les réseaux et applications physiques et logiques;
- 7.4.12. Examiner et analyser les journaux de sécurité aux fins des événements de sécurité dans le but de concevoir des garanties et des contre-mesures;
- 7.4.13. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT;
- 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).

7.5. C.9 – Opérateur de systèmes de sécurité des TI, niveau 3

Les opérateurs de systèmes de sécurité des technologies de l'information de niveau 3 doivent :

- 7.5.1. Créer des échéanciers et des plans de travail;
- 7.5.2. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, notamment :
 - 7.5.2.1. normes d'annuaire comme X.500 et LDAP;

- 7.5.2.2. protocoles réseau comme HTTP, FTP et Telnet;
- 7.5.2.3. protocoles de sécurité Internet (TSL, HTTPS, S-MIME, IPSec, SSH);
- 7.5.2.4. protocoles comme TCP/IP, UDP, DNS, SMTP et autres protocoles applicables;
- 7.5.2.5. routeurs, multiplexeurs et commutateurs réseau;
- 7.5.2.6. techniques de renforcement des réseaux, notamment procédure d'interpréteur de commandes [shell scripting], identification des services et contrôle des accès);
- 7.5.2.7. algorithmes cryptographiques approuvés par le gouvernement;
- 7.5.2.8. mesures de protection techniques des TI;
- 7.5.2.9. technologie sans fil.
- 7.5.3. Déceler les menaces techniques pesant sur les réseaux et leurs vulnérabilités;
- 7.5.4. Configurer ou administrer les systèmes d'exploitation, comme MS, Unix et Linux;
- 7.5.5. Configurer et surveiller les systèmes de détection/prévention d'intrusion, les coupe-feu et les vérificateurs de contenu;
- 7.5.6. Extraire des données des rapports et des registres et les analyser, et répondre aux incidents en matière de sécurité;
- 7.5.7. Configurer et mettre à jour les détecteurs de virus;
- 7.5.8. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT;
- 7.5.9. Élaborer et fournir une trousse de matériel de formation en matière de sensibilisation à la sécurité des TI;
- 7.5.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.6. <u>C.3 – Analyste, Certification et accréditation (C et A) pour l'Évaluation de la menace et</u> des risques (EMR) en matière de sécurité des TI, niveau 3

Les analystes, Certification et accréditation (C et A) pour l'Évaluation de la menace et des risques (EMR) en matière de sécurité des TI, niveau 3 doivent :

- 7.6.1. Créer des échéanciers et des plans de travail;
- 7.6.2. Effectuer des examens et des analyses et veiller au respect :
 - 7.6.2.1. des politiques fédérales, provinciales et territoriales sur la sécurité des TI;
 - 7.6.2.2. des processus relatifs aux systèmes de C et A en sécurité des TI;
 - 7.6.2.3. des produits, des mesures de protection et des pratiques exemplaires pour la sécurité des TI;
 - 7.6.2.4. des stratégies d'atténuation des risques liés à la sécurité des TI;
- 7.6.3. Examiner et déterminer :
 - 7.6.3.1. les menaces à l'égard des systèmes d'exploitation comme Microsoft (MS), Unix et Novell et les vulnérabilités de ceux-ci;
 - 7.6.3.2. les menaces à l'égard des architectures sans fil et les vulnérabilités de celles-ci;

- 7.6.3.3. les menaces de diverses natures (personnelle, technique, procédurale) et les vulnérabilités à l'égard des systèmes de TI fédéraux, provinciaux et territoriaux;
- 7.6.4. Analyser et réaliser :
 - 7.6.4.1. des analyses sur la sécurité des données;
 - 7.6.4.2. des contrôles de sécurité;
 - 7.6.4.3. des concepts d'opération (CONOP);
 - 7.6.4.4. des énoncés de sensibilité;
 - 7.6.4.5. des évaluations des menaces:
 - 7.6.4.6. des évaluations des facteurs relatifs à la vie privée (EFVP);
 - 7.6.4.7. des évaluations non techniques de la vulnérabilité;
 - 7.6.4.8. des évaluations des risques;
 - 7.6.4.9. des réunions d'information sur les menaces, les vulnérabilités ou les risques en matière de sécurité des TI:
- 7.6.5. Effectuer des tâches liées à la certification telles :
 - 7.6.5.1. l'élaboration de plans de certification;
 - 7.6.5.2. la vérification de la conformité des mécanismes de sécurité aux politiques et normes applicables;
 - 7.6.5.3. la validation des exigences de sécurité en mettant en correspondance la politique de sécurité propre au système et les exigences de fonctionnalité de sécurité et en faisant le suivi des exigences de sécurité tout au long de la préparation des spécifications du système;
 - 7.6.5.4. la vérification des mesures de protection pour s'assurer qu'elles ont été aménagées correctement et qu'elles offrent l'assurance voulue. Cela comprend la confirmation que le système a été correctement configuré et la mise en place de mesures de protection qui satisfont aux normes applicables;
 - 7.6.5.5. les essais et évaluations de sécurité visant à déterminer si les mesures de protection techniques fonctionnent correctement;
 - 7.6.5.6. l'évaluation des risques résiduels mis au jour par l'évaluation des risques (consulter la section 6.6.4.8) afin de déterminer si le niveau de risque est acceptable;
- 7.6.6. Effectuer des tâches liées à l'accréditation telles :
 - 7.6.6.1. l'examen, par l'autorité d'accréditation, des résultats de la certification reproduits dans les documents d'examen conceptuel fournis, pour s'assurer que les risques entourant l'exploitation du système seront acceptables et que ce dernier respectera les politiques et normes de sécurité pertinentes du Ministère et celles qui lui sont propres;

- 7.6.6.2. la détermination des conditions dans lesquelles le système devra fonctionner (aux fins d'approbation). Cela peut comprendre les formes d'autorisation du MDN suivantes :
 - 7.6.6.2.1. l'autorisation d'élaboration, donnée de concert par l'exploitant et par l'autorité d'accréditation, de passer à l'étape d'élaboration suivante dans le cycle de vie du système de TI si celui-ci doit traiter des renseignements de nature délicate pendant son élaboration;
 - 7.6.6.2.2. l'autorisation d'exploitation, donnée par écrit, pour autoriser l'exploitation du système de TI mis en place, de même que le traitement de renseignements de nature délicate, lorsque les risques assortis à l'exploitation du système sont jugés acceptables et que le système respecte les normes et politiques de sécurité pertinentes;
 - 7.6.6.2.3. l'autorisation provisoire, également donnée par écrit, pour autoriser le traitement de renseignements de nature délicate dans des circonstances particulières, lorsqu'on n'a pas encore réussi à ramener les risques à un niveau acceptable, mais qu'il est nécessaire d'exploiter le système en cours d'élaboration:
- 7.6.7. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.6.8. Élaborer et fournir une trousse de matériel de formation pertinente à la C et A et à l'ÉMR en matière de sécurité des TI;
- 7.6.9. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

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

Les spécialistes des analyses de vulnérabilité de la sécurité des technologies des TI de niveau 3 doivent :

- 7.7.1. Créer des échéanciers et des plans de travail;
- 7.7.2. Examiner, analyser et évaluer divers outils d'analyse des agents de menace et technologies émergentes et prodiguer des conseils à leur égard, notamment :
 - 7.7.2.1. la protection des renseignements personnels, l'analyse prédictive, la VoIP, la visualisation et la fusion des données;
 - 7.7.2.2. les dispositifs de sécurité sans fil, PBX et le coupe-feu pour téléphonie;
 - 7.7.2.3. les détecteurs d'accès entrant et les perceurs de mots de passe;
 - 7.7.2.4. les services consultatifs publics en matière de vulnérabilité des TI;
 - 7.7.2.5. les analyseurs de réseau et outils d'analyse des vulnérabilités comme le logiciel SATAN (Security Administrator Tool for Analysing Networks), le soutien en service (ISS), Portscan, KALI et NMap;

- 7.7.3. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, notamment :
 - 7.7.3.1. protocoles réseau comme HTTP, FTP et Telnet;
 - 7.7.3.2. protocoles de sécurité Internet (TSL, HTTPS, S-MIME, IPSec, SSH);
 - 7.7.3.3. protocoles comme TCP/IP, UDP, DNS, SMTP et autres protocoles applicables;
 - 7.7.3.4. sécurité sans fil;
 - 7.7.3.5. systèmes de détection/prévention d'intrusion, coupe-feu, logiciels antivirus et vérificateurs de contenu:
- 7.7.4. Déceler les menaces techniques pesant sur les réseaux et leurs vulnérabilités;
- 7.7.5. Réaliser des examens et des analyses sur place des registres de sécurité des systèmes;
- 7.7.6. Recueillir, examiner et évaluer de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents, avant de diffuser l'information et l'analyse à la cybersécurité du MDN;
- 7.7.7. Documenter et tenir des réunions d'information sur les menaces, les vulnérabilités ou les risques liés à la sécurité des TI;
- 7.7.8. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.7.9. Élaborer et fournir une trousse de matériel de formation en matière d'analyse de vulnérabilité de la sécurité des TI;
- 7.7.10. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

7.8. C.12 - Spécialiste de la gestion des incidents, niveau 3

Le spécialiste en gestion des incidents de niveau 3 doit :

- 7.8.1. Créer des échéanciers et des plans de travail;
- 7.8.2. Examiner, analyser, évaluer les éléments suivants et prodiguer des conseils à leur égard :
 - 7.8.2.1. analyseurs de réseau et outils d'analyse des vulnérabilités comme le logiciel SATAN (Security Administrator Tool for Analysing Networks), le soutien en service (ISS), Portscan, KALI et NMap;
 - 7.8.2.2. procédures de rapport et de résolution des incidents de sécurité des TI (p. ex., attaque par déni de service) et services-conseils internationaux en matière d'incidents de sécurité des TI;
- 7.8.3. Examiner, analyser, évaluer diverses technologies de la sécurité et prodiguer des conseils à leur égard, notamment :
 - 7.8.3.1. protocoles réseau comme HTTP, FTP et Telnet;

- 7.8.3.2. protocoles de sécurité Internet (TSL, HTTPS, S-MIME, IPSec, SSH);
- 7.8.3.3. protocoles comme TCP/IP, UDP, DNS, SMTP et autres protocoles applicables;
- 7.8.3.4. systèmes de détection d'intrusion, coupe-feu, logiciels antivirus et vérificateurs de contenu:
- 7.8.3.5. routeurs, multiplexeurs et commutateurs réseau;
- 7.8.4. Assurer un soutien pour l'analyse des incidents, notamment :
 - 7.8.4.1. les mécanismes d'intervention;
 - 7.8.4.2. la coordination de tous les plans de prévention et d'intervention;
 - 7.8.4.3. les activités du Centre des opérations d'urgence (COE);
 - 7.8.4.4. la coordination avec le Centre intégré d'évaluation des menaces à l'échelle nationale et le Centre des opérations du gouvernement;
 - 7.8.4.5. la participation ou la contribution au cadre de sécurité nationale intégré et à la stratégie nationale de cybersécurité;
- 7.8.5. Recueillir, examiner et évaluer de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents, avant de diffuser l'information et l'analyse à la cybersécurité du MDN;
- 7.8.6. Réaliser des examens et des analyses sur place des registres de sécurité des systèmes;
- 7.8.7. Générer des rapports d'activité et des registres des activités et des analyses des incidents:
- 7.8.8. Régler les problèmes signalés au centre de réponse aux incidents et aider à l'administration du centre;
- 7.8.9. Participer aux réunions et aux groupes de travail hebdomadaires, à la demande du RT:
- 7.8.10. Élaborer et fournir une trousse de matériel de formation en matière de gestion des incidents:
- 7.8.11. Effectuer d'autres tâches désignées par le RT liées à cette catégorie professionnelle des Services professionnels en informatique centrés sur les tâches (SPICT).

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. Tous les rapports d'étape doivent 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 la réalisation 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. Toute recommandation visant la mise à jour des 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 effectués dans les installations du MDN, dans la RCN.

11. DÉPLACEMENTS

- 11.1. Les frais de déplacement au sein de la région 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.

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

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 utilisant les tableaux fournis dans la présente annexe. Aux fins de l'établissement des grilles de ressources, les soumissionnaires devraient fournir Pour faciliter l'évaluation des ressources, les entrepreneurs doivent préparer et soumettre leur réponse à un projet d'autorisation de tâches en vitæ. Seule la réponse demandée devrait être fournie.

CRITÈRES OBLIGATOIRES

P.1 Conseiller en gestion du changement – Niveau 3

1.1	r.1 Conseiner en gestion un changement – Myeau 3	- Miveau 3		
	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
			RESPECTÉE	RESPECTÉE PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
Р.	P.1 Conseiller en gestion du changement – Niveau 3	– Niveau 3		
0	O1 L'entrepreneur doit prouver que la			
	ressource proposée possède : soit au moins			
	dix (10) années d'expérience combinée à			
	titre de conseiller en gestion du			
	changement au cours des			
	quinze (15) dernières années, soit au			
	moins (5) années d'expérience à titre de			
	conseiller en gestion du changement au			
	cours des dix (10) dernières années			
	accompagnées d'au moins trois (3) des			
	accréditations professionnelles reconnues			
	des suivantes :			
	 Association of Change Management 			
	Professionals (Association des			
	professionnels de la gestion du			
	changement);			

Niveau 3
et –
proj
de
tionnaire
Ges
P.9

RESPECTÉE	NON COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)			
		P.9 Gestionnaire de projet – Niveau 3	L'entra ressou dix (1 titre d des ques que moins gestio dix (1 trois (recom r	ressource doit être jointe à la soumission.

	00	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans la planification, l'évaluation, le suivi et la supervision d'activités d'une équipe de projet, ainsi que la formulation de conseils à cet égard.		
<u> </u>	03	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience acquise au cours des dix (10) dernières années dans l'élaboration et la tenue à jour de plans de projet, d'échéanciers, de coûts et de ressources à l'aide de Microsoft Project 2013 (ou d'une version plus récente).		
		Conforme (oui/non)?		

C.5 Spécialiste de l'ICP – Niveau 2

	TALLENGE	DECDECTÉE	NON	COMMENTATORS (FINDBOTT DANS I A
			TÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C	C.5 Spécialiste de l'ICP – Niveau 2			
01	L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	cinq (5) années d'expérience acquise au			
	cours des dix (10) dernieres années dans			
	solutions d'ICP.			
02	L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	deux (2) années d'expérience combinée			
	dans la rédaction d'au moins deux (2)			
	des types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception 			
	du système;			
	 documents sur la conception et 			
	la configuration;			
	 concept d'opération (CONOP); 			
	 plans de mise en œuvre de 			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

C.5 Spécialiste de l'ICP – Niveau 3

,			MOM	
	EXIGENCE	KESPECIEE	NON RESPECTÉE	COMMEN LAIKES (ENDROLL DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C	C.5 Spécialiste de l'ICP – Niveau 3			
01				
	ressource proposée possède au moins			
	dix (10) années d'expérience acquise au			
	cours des quinze (15) dernières années			
	dans la mise en œuvre et le soutien de			
02	2 L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	trois (3) années d'expérience combinée			
	dans la rédaction d'au moins trois (3) des			
	types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception 			
	du système;			
	 documents sur la conception et 			
	la configuration;			
	• CONOP;			
	 plans de mise en œuvre de 			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	Conforme (oui/non)?			

		The state of the s		TA DIET G MAC GGIRLY DIGGIT MIXES TO SOO
	EXIGENCE	KESPECTEE	NON	COMMENTAIRES (ENDROIT DANS LA
			KESFECIEE	PROPOSITION, CRITERES NON SATISFALIS, ETC.)
)	C.6 Ingénieur en sécurité des TI – Nive	Viveau 1		
	ressource proposée possède au moins une (1) année d'expérience acquise au cours des cinq (5) demières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants : Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.			

O2 L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.		EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
L'entrep ressource une (1) a dans la r des types systèmes systèmes				RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
ressource proposée possède au moins une (1) année d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.)2	L'entrepreneur doit démontrer que la			
une (1) année d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.		ressource proposée possède au moins			
dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.		une (1) année d'expérience combinée			
des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.		dans la rédaction d'au moins deux (2)			
 systèmes suivants: spécifications de la conception du système; documents sur la conception et la configuration; CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		des types de documents d'ingénierie des			
 spécifications de la conception du système; documents sur la conception et la configuration; CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		systèmes suivants:			
du système; documents sur la conception et la configuration; CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie.		 spécifications de la conception 			
 documents sur la conception et la configuration; CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		du système;			
la configuration; CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie.		 documents sur la conception et 			
 CONOP; plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		la configuration;			
 plans de mise en œuvre de systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		• CONOP;			
 systèmes; plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		• plans de mise en œuvre de			
 plans et rapports de mises à l'essai; plans de soutien du cycle de vie. Conforme (oui/non)?		systèmes;			
Pessai; plans de soutien du cycle de vie. Conforme (oui/non)?		 plans et rapports de mises à 			
plans de soutien du cycle de vie. Conforme (oui/non)?		l'essai;			
Conforme (oni/non)?		 plans de soutien du cycle de vie. 			
Conforme (oni/non)?					
		Conforme (oui/non)?			

C.6 Ingénieur en sécurité des TI – Niveau 2

	0		111111111111111111111111111111111111111	
	EXIGENCE	RESPECTEE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
Ü	C.6 Ingénieur en sécurité des TI – Niv	Niveau 2		
	L'entrepreneur doit demontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants: Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.			

	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)		
EXIGENCE L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de l'essai; • plans de soutien du cycle de vie. Conforme (oui/non)?	NON RESPECTÉE		
EXIGE L'entrep ressource deux (2) dans la r das types systèmes .	RESPECTÉE		
05	EXIGENCE	L'entrep ressource deux (2) dans la ry des types systèmes	Conforme (oui/non)?
		00	

ĺ				
	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION CRITÈRES NON SATISFAITS ETC.)
				INCLOSITION, CALIFORNIA INCLOSITISTATIS, ETC.)
C.C	C.6 Ingénieur en sécurité des TI – Nive	liveau 3		
j	L'entrepreneur doit demontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants : Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.			

COMMENTAIRES (ENDROIT DANS LA	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)																	
NON	RESPECTÉE																	
RESPECTÉE																		
EXIGENCE		L'entrepreneur doit démontrer que la	ressource proposée possède au moins	trois (3) années d'expérience combinée	dans la rédaction d'au moins trois (3) des	types de documents d'ingénierie des	systèmes suivants :	 spécifications de la conception 	du système;	 documents sur la conception et 	la configuration;	• CONOP;	• plans de mise en œuvre de	systèmes;	 plans et rapports de mises à 	l'essai;	 plans de soutien du cycle de vie. 	Conforme (oui/non)?
		02																

C.7 Spécialiste en conception de sécurité des TI – Niveau 2

	EXICENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
			ÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C:	C.7 Spécialiste en conception de sécurité des TI – Niveau 2	ité des TI – Niv	eau 2	
01	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au			
	cours des dix (10) dernières années dans la planification et la mise en œuvre			
	d'architectures d'intégration de la			
02	L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	deux (2) années d'expérience combinée			
	dans la rédaction d'au moins deux (2)			
	des types de documents d'ingénierie des			
	systèmes suivants :			
	• spécifications de la conception			
	du systeme;			
	 documents sur la conception et 			
	la configuration;			
	• CONOP;			
	 plans de mise en œuvre de 			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	Conforme (oui/non)?			

	ar mana ar	2137 77 77 77 7	3	
	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C;	C.7 Spécialiste en conception de sécurité des TI – Niveau 3	té des TI – Niv	eau 3	
01	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans la planification et la mise en œuvre d'architectures d'intégration de la sécurité des TI.			
00	L'entrepreneur doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée dans la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

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

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
		!	lée	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C.8	C.8 Analyste de la sécurité des réseaux – Niveau 2	– Niveau 2		
10	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans l'examen, l'analyse, la mise en œuvre et le soutien d'au moins une (1) des technologies suivantes: • protocoles de sécurité Internet; • protocoles réseau; • algorithmes cryptographiques; • normes d'amuaire; • renforcement de la sécurité réseau; • resforcement de la sécurité réseau;			

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
00	L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience acquise au cours des cinq (5) dernières années dans l'élaboration d'exigences et la conception d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants : Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.			
	Conforme (oui/non)?			

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

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
			RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
ິວິ	C.8 Analyste de la sécurité des réseaux – Niveau 3	. – Niveau 3		
01	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins une (1) des technologies suivantes: • protocoles de sécurité Internet; • protocoles réseau; • algorithmes cryptographiques; • normes d'annuaire; • renforcement de la sécurité réseau; • réseau;			

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
00	L'entrepreneur doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans l'élaboration d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants : • Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); • Technologies de sécurité de réseautage sans fil; • Systèmes de détection d'intrusion (IDS); • Systèmes de prévention des intrusions dans un réseau (IPS); • Gestion de l'information et des incidents de sécurité (SIEM); • Gestion de l'information et des incidents de l'accès au réseau (NAC); • Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou • Protection des terminaux.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

P.1 Conseiller en gestion du changement – Niveau 3

°	N° CRITÈRES	BAREME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
P.1 C	Conseiller en gestion du change	ment – Niveau 3			
CI	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de documents de gestion de projet à l'aide des lignes directrices du Project Management Body of Knowledge (référentiel des connaissances en gestion de projet).	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C2	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la gestion de l'information au moyen d'un outil, comme SharePoint.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C3	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la direction et l'animation de réunions, de groupes de travail et de discussions, ainsi que dans la préparation d'exposés et leur présentation à divers intervenants.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C4	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la conduite d'analyses des répercussions du changement et d'activités de gestion du changement.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)			
NOTE					
MAX.	DE	POINTS	4		Note maximale: 24 points
BARÈME DE NOTATION			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 8 années d'expérience 4 points = plus de 8 années d'expérience 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 8 années d'expérience 4 points = plus de 8 années d'expérience	Note de passage minimale : 14 points
N° CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la gestion d'autres employés afin de définir les stratégies et les processus opérationnels permettant de favoriser les transformations et les d'expérience	l'expérience dans la réalisation de vérifications des processus de gestion de la configuration et du changement.	Total:
$\overset{\circ}{\mathbf{Z}}$			90		

S.N.	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET PARAGRAPHE)
P.9 G	Gestionnaire de projet – Niveau	3 1 moint - de 1 à 3 années d'avnérience			
5		1 point – de 1 a 3 annees d'experience 2 aointe – alue de 2 à 5 années	t		
		2 points – pius uc 3 a 3 aimees d'exnérience			
		3 points = plus de 5 à 8 années			
		d'expérience			
	1)	4 points = plus de 8 années			
	l'équipe de projet connexe.	d'expérience			
C2	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
		d'expérience			
	documents de gestion de projet à	3 points = plus de 5 à 8 années			
	l'aide des lignes directrices du	d'expérience			
	Jo	4 points = plus de 8 années			
	Knowledge (référentiel des	d'expérience			
	connaissances en gestion de projet).				
C3	L'entrepreneur doit démontrer que	3 projets = 1 point	4		
	la ressource proposée a acquis, au	4 projets = 2 points			
	cours des cinq (5) dernières années,	5 projets = 3 points			
	de l'expérience dans la gestion de	6 projets = 4 points			
	projets de GI-TI aux phases				
	d'élaboration ou de mise en œuvre à				
	l'aide de Microsoft Project afin de				
	garantir que les ressources sont				
	disponibles et que le projet est				
	conçu et entièrement fonctionnel.				
	Pour être price en compte				
	l'expérience doit avoir été d'au				
	moins six (6) mois.				

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
22	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, de l'expérience dans la détermination et la documentation des jalons des projets de GI-TI, la détermination des exigences budgétaires, la constitution d'équipes de projet, ainsi que la définition des rôles, des responsabilités et du mandat des membres des équipes. Pour être prise en compte, l'expérience doit avoir été d'au moins six (6) mois.	3 projets = 1 point 4 projets = 2 points 5 projets = 3 points 6 projets = 4 points	4		
S	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la gestion de l'information au moyen d'un outil, comme SharePoint.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
CG	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la direction et l'animation de réunions, de groupes de travail et de discussions, ainsi que dans la préparation d'exposés et leur présentation à divers intervenants.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

TE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)																	
NOTE																			
MAX.	DE	POINTS	4							4							Note	maximale:	32 points
BARÈME DE NOTATION			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 8 années	d'expérience	4 points = plus de 8 années	d'expérience	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 8 années	d'expérience	4 points = plus de 8 années	d'expérience	Note minimale de passage :	19 points	
CRITÈRES			L'entrepreneur doit démontrer que	la ressource proposée a de	l'expérience en matière	d'élaboration et de gestion d'un	plan d'activités.			L'entrepreneur doit démontrer que	la ressource proposée possède de	l'expérience dans le lancement et la	gestion de l'approvisionnement,	ainsi que la gestion de contrat de	sécurité des TI.		Total:		
$\overset{\circ}{\mathbf{Z}}$			C2							C8									

24/51

C.5 Spécialiste de l'ICP – Niveau 2

combinée démontrée avec quatre (4)
des technologies enoncees dans un contexte d'ICP 5 points = minimum d'expérience combinée démontrée avec cinq (5) ou plus des technologies énoncées dans un contexte d'ICP

NOTE RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)		
MAX. No DE POINTS	4	4
BARÈME DE NOTATION	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	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
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience combinée dans les éléments suivants: 1) élaboration de politiques de certification pour l'ICP; 2) élaboration d'énoncés de pratiques de certification pour l'ICP; 3) vérifications et inspections de la conformité à la politique de certification pour l'ICP.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience combinée dans la rédaction des documents d'ingénierie suivants liés à l'ICP: 1) architectures de solutions; 2) les spécifications de la conception du système; 3) les analyse d'options; 4) les procédures opérationnelles normalisées (PON); 5) les mesures de rendement des systèmes et de la planification de la capacité; 6) les plans de continuité des activités et de reprise après sinietre
$\overset{\circ}{\mathbf{Z}}$	23	ប

° Z

7

6

CS

3

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION MAX. NOTE RÉFÉRENCE À LA	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

28/51

C.5 Spécialiste de l'ICP – Niveau 3

°Z	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.5 S	C.5 Spécialiste de l'ICP – Niveau 3				
C1	L'entrepreneur doit démontrer que	1 point = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec une (1) des			
	moins cinq (5) années d'expérience	technologies énoncées dans un			
	combinée dans l'examen, l'analyse,	contexte d'ICP			
	la mise en œuvre et le soutien des	2 points = minimum d'expérience			
	technologies suivantes dans un	combinée démontrée avec deux (2)			
	contexte d'ICP:	des technologies énoncées dans un			
		contexte d'ICP			
	1) architectures d'ICP;	3 points = minimum d'expérience			
	2) signatures numériques et	combinée démontrée avec trois (3)			
	chiffrement;	des technologies énoncées dans un			
	3) produits d'ICP, notamment	contexte d'ICP			
	l'autorité de certification et	4 points = minimum d'expérience			
	l'autorité d'enregistrement;	combinée démontrée avec quatre (4)			
	4) produits reposant sur des clés	des technologies énoncées dans un			
	publiques, comme les réseaux	contexte d'ICP			
	privés virtuels, la voix par le	5 points = minimum d'expérience			
	protocole Internet et l'extension	combinée démontrée avec cinq (5) ou			
	S/MIME;	plus des technologies énoncées dans			
	5) produits d'annuaire X.500;	un contexte d'ICP			
	6) normes de certificat X.509;				
	7) protocoles de sécurité Internet;				
	8) produits du protocole de				
	vérification en ligne de l'état des				
	certificats.				

°	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C2	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
	l'expérience combinée dans les	d'expérience			
	éléments suivants :	3 points = plus de 5 à 8 années			
	;	d'experience			
	1) élaboration de politiques de	4 points = plus de 8 années			
	certification pour l'ICP;	d'expérience			
	2) élaboration d'énoncés de				
	pratiques de certification pour				
	l'ICP;				
	3) vérifications et inspections de la				
	conformité à la politique de				
	certification pour l'ICP.				
C3	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
	l'expérience combinée dans la	d'expérience			
	rédaction des documents	3 points = plus de 5 à 8 années			
	d'ingénierie suivants liés à l'ICP :	d'expérience			
		4 points = plus de 8 années			
	1) les architectures de solutions;	d'expérience			
	2) les spécifications de la				
	conception du système;				
	3) les analyse d'options;				
	4) les procédures opérationnelles				
	normalisées (PON);				
	5) les mesures de rendement des				
	systèmes et de la planification				
	de la capacité;				
	6) les plans de continuité des				
	activités et de reprise après				
	sinistre.				

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C4	L'entrepreneur doit démontrer que la ressource proposée a travaillé pendant au moins cinq (5) années avec les produits/solutions d'ICP cidessous: 1) autorité de certification Entrust; 2) autorité de certification Microsoft; 3) modules de sécurité matérielle; 4) solutions de gestion des cartes; 5) cartes à puce et logiciels des cartes à puce; 6) logiciel client Entrust.	I point = minimum d'expérience combinée démontrée avec un (1) des produits/solutions d'ICP énumérés 2 points = minimum d'expérience combinée démontrée avec deux (2) des produits/solutions d'ICP énumérés 3 points = minimum d'expérience combinée démontrée avec trois (3) des produits/solutions d'ICP énumérés 4 points = minimum d'expérience combinée démontrée avec quatre (4) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec quatre (5) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec cinq (5) ou plus des produits/solutions d'ICP énumérés	S		
CS	L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CSSP); 3) Systems Security Certified Professional (SSCP); Une copie des certifications valides de la ressource doit être jointe à la soumission.	2 points = preuve d'au moins une des certifications énumérées	2		

$^{\circ}$	CRITÈRES	BARÈME DE NOTATION MAX. NOTE RÉFÉRENCE À LA	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

C.6 Ingénieur en sécurité des TI – Niveau 1

	or migrification securite and it	T mm T		- 1	
$\overset{\circ}{\mathbf{Z}}$	CRITERES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.61	Ingénieur en sécurité des TI – Ni	Niveau 1			
C1	L'entrepreneur doit démontrer que	1 point = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec une (1) des			
	moins une (1) année d'expérience	solutions de sécurité des TI			
	combinée de l'élaboration et de la	énumérées			
	documentation de spécifications	2 points = minimum d'expérience			
	relatives aux exigences de système	combinée démontrée avec deux (2)			
	pour les solutions en matière de	des solutions de sécurité des TI			
	sécurité des TI suivantes :	énumérées			
		3 points = minimum d'expérience			
	1) Systèmes de prévention des	combinée démontrée avec trois (3)			
	intrusions au niveau de	des solutions de sécurité des TI			
	l'hôte (HIPS);	énumérées			
	2) Technologies de sécurité	4 points = minimum d'expérience			
	de réseautage sans fil;	combinée démontrée avec quatre (4)			
	3) Systèmes de détection	des solutions de sécurité des TI			
	d'intrusion (IDS);	énumérées			
	4) Systèmes de prévention des	5 points = minimum d'expérience			
	intrusions dans un réseau	combinée démontrée avec cinq (5)			
	(IPS);	des solutions de sécurité des TI			
	5) Gestion de l'information et	énumérées			
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	9) Protection des terminaux.				

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
MAX.	DE	POINTS	κ	33	ĸ	Note maximale : 14 points
BARÈME DE NOTATION		P	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	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	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.	Note de passage minimale : 8 points Note maxi maxi
CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.	Total:
$\overset{\circ}{\mathbf{Z}}$			C3	C3	75	

C.6 Ingénieur en sécurité des TI – Niveau 2

°Z	CRITTERES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
l			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6 I	C.6 Ingénieur en sécurité des TI – Ni	- Niveau 2			
C1	L'entrepreneur doit démontrer que	1 point = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec une (1) des			
	moins deux (2) années d'expérience	solutions de sécurité des TI			
	combinée de l'élaboration et de la	énumérées			
	documentation de spécifications	2 points = minimum d'expérience			
	relatives aux exigences de système	combinée démontrée avec deux (2)			
	pour les solutions en matière de	des solutions de sécurité des TI			
	sécurité des TI suivantes :	énumérées			
		3 points = minimum d'expérience			
	ı des	combinée démontrée avec trois (3)			
	intrusions au niveau de	des solutions de sécurité des TI			
	l'hôte (HIPS);	énumérées			
	2) Technologies de sécurité de	4 points = minimum d'expérience			
	réseautage sans fil;	combinée démontrée avec quatre (4)			
	3) Systèmes de détection	des solutions de sécurité des TI			
	d'intrusion (IDS);	énumérées			
	4) Systèmes de prévention des	5 points = minimum d'expérience			
	intrusions dans un réseau	combinée démontrée avec cinq (5)			
	(IPS);	des solutions de sécurité des TI			
	5) Gestion de l'information et	énumérées			
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	9) Protection des terminaux.				

E RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)			
NOTE			
MAX. DE POINTS	4	4	4
BARÈME DE NOTATION	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	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	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
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.
$^{\circ}\mathbf{Z}$	C2	C3	C4

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)						
MAX. N	DE	POINTS	0			•	maximale:	19 points
	_	PO				Note	maxi	19 pc
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées			Note de passage minimale :	11 points	
N° CRITÈRES			L'entrepreneur doit démontrer que 2 points = preuve d'au m la ressource proposée détient une (1) certifications énumérées des certifications suivantes : 1) professionnel agréé en sécurité des systèmes d'information; 2) Certified Cloud Security Professional (professionnel	agrée en sécurité de l'informatique en nuage); 3) professionnel agrée en sécurité des systèmes.	Une copie des certifications valides de la ressource doit être jointe à la soumission.	Total:		
$\overset{\circ}{\mathbf{Z}}$			ప					

C.6 Ingénieur en sécurité des TI – Niveau 3

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)			
NOTE			
MAX. DE POINTS	4	4	4
BARÈME DE NOTATION	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.
\mathbf{Z}°	C3	<u>:</u>	C4

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)											
NOTE													
MAX.	DE	POINTS	7								Note	maximale:	19 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées								Note de passage minimale :	11 points	
CRITÈRES			L'entrepreneur doit démontrer que la ressource détient une (1) des certifications suivantes :	1) Certified Information System	Security Professional (CISSP);	2) Certified Cloud Security Professional (CCSD): and/or	3) Systems Security Certified	Professional (SSCP);	Une copie des certifications valides	de la ressource doit être jointe à la	Total:		
$\overset{\circ}{\mathbf{Z}}$			C5										

C.7 Spécialiste en conception de sécurité des TI – Niveau 2

ol V	O COLLEGE OF A DEVICE NOT	PADEME DE NOTATION	MAV	ACT	DÉPÉDENCE À I A
7		DANEME DE NOTATION	DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.7S	C.7 Spécialiste en conception de sécurité des TI – Niveau 2	ırité des TI – Niveau 2			
Cl	L'entrepreneur doit démontrer que	1 point = de 1 à 2 années d'expérience	3		
	la ressource proposee possede l'expérience de l'application des	z points = pius de z a 3 annees d'expérience			
	politiques du gouvernement en	3 points = plus de 3 années			
	matière de sécurité des TI à la	d'expérience.			
	rédaction d'un document de				
	planification, d'analyse ou de mise				
\mathcal{C}	I 'entreprenent doit démontrer que	1 noint - de 1 à 2 années d'avnérience	_		
1	10 recontros nocedas de 1º evnárionos	1 point – uv 1 a 2 annives a vaperirumo	r		
	combinée dans l'analyse d'an moins	z ponns – prus ue z a 3 annees d'exnérience			
	combine dans ranaryse a administra (1) des éléments enivants.	a capetitude 3 points — plus de 3 à 4 années			
		d'expérience			
	1) outils et techniques de sécurité	4 points $=$ plus de 4 années			
	des TI:	d'expérience			
	2) données de sécurité et				
	nrésentation d'avis et de				
	rapports:				
	3) statistiques sur la sécurité des				
	, TI.				
C3	L'entrepreneur doit démontrer que	1 point = de 1 à 2 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 2 à 3 années			
	l'expérience dans la classification	d'expérience			
	ou la désignation du niveau de	3 points = plus de 3 à 4 années			
	sécurité des données.	d'expérience			
		4 points = plus de 4 années			
		n expensione			

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		11 points	maximale:		
			19 points		

C.7 Spécialiste en conception de sécurité des TI – Niveau 3

NIO N	Correpose	NOTATION OF TAXABLA	MAN	NOTE	DÉPÉPENCE À I A
	CRITERES	DAREME DE NOTATION	MAA.	NOIE	KEFEKENCE A LA
			DE		PROPOSITION (PAGE ET
.7 S	Spécialiste en conception de sécu	écurité des TI – Niveau 3	CINIOI		I AINAGINAL IIIE)
5	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans l'application des politiques du gouvernement en matière de sécurité des TI à la rédaction des documents d'ingénierie des systèmes (conception, réalisation, essai et mise en œuvre) ou à la mise en œuvre d'une solution.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
2	L'entrepreneur doit démontrer que la ressource possède de l'expérience combinée dans l'analyse d'au moins un (1) des éléments suivants : 1) outils et techniques de sécurité des TI; 2) données de sécurité et présentation d'avis et de rapports; 3) statistiques sur la sécurité des 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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
ප	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans les études de classification ou de désignation du niveau de sécurité des données.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			POINTS		FROFOSITION (FAGE E1 PARAGRAPHE)
^C 4	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience combinée dans la rédaction d'au moins un des rapports techniques suivants: 1) analyse des besoins; 2) analyse des options; 3) documents d'architecture technique; 4) modélisation mathématique des risques.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
S	L'entrepreneur doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes: 1) Microsoft Certified Architect (MCA); 2) VMware Certified Design Expert (VCDX); 3) Microsoft Certified System Engineer (MCSE); 4) Certified Information System Security Professional (CISSP); 5) Certified Cloud Security Professional (CSSP); 6) Certified CSSP); et/ou 6) Systems Security Certified Professional (SSCP); Une copie des certifications valides de la ressource doit être jointe à la soumission.	2 points = preuve d'au moins une (1) des certifications énumérées 4 points = preuve d'au moins deux (2) des certifications énumérées	4		

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION MAX.	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

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

01/2	No Correspec	PADÈME DE NOTATION	MAN	NOTE	DÉPÉPENCE À I A
		DANEME DE NOTATION	INTEG.		NEFEMENCE A LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.8	C.8 Analyste de la sécurité des réseaux – Niveau 2	ux – Niveau 2			
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins une (1) année d'expérience	des solutions de sécurité des TI			
	combinée dans l'examen, l'analyse	énumérées			
	et la mise en œuvre d'au moins	3 points = minimum d'expérience			
	deux (2) des solutions en matière de	combinée démontrée avec trois (3)			
	sécurité des suivantes :	des solutions de sécurité des TI			
		énumérées			
	1) protocoles de sécurité Internet;	4 points = minimum d'expérience			
	2) protocoles réseau;	combinée démontrée avec quatre (4)			
	3) algorithmes cryptographiques;	des solutions de sécurité des TI			
	4) normes d'annuaire;	énumérées			
	5) renforcement de la sécurité	5 points = minimum d'expérience			
	réseau;	combinée démontrée avec cinq (5)			
	6) systèmes d'exploitation.	des solutions de sécurité des TI			
		énumérées			

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)	
NOTE	
MAX. DE POINTS	5
BARÈME DE NOTATION	3 points = minimum d'expérience combinée démontrée dans trois (3) des domaines énumérés 4 points = minimum d'expérience combinée démontrée dans quatre (4) des domaines énumérés 5 points = minimum d'expérience combinée démontrée dans cinq (5) ou plus des domaines énumérés
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience dans l'élaboration d'exigences et la conception d'applications et d'infrastructures de sécurité des TI dans au moins trois (3) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS); 5) Gestion de l'information et des incidents de sécurité (SIEM); 6) Saisie intégrale de paquet (FPC); 7) Contrôle de l'accès au réseau (NAC); 8) Gestion de l'identité et de l'accès (ICAM); et/ou 9) Protection des terminaux.
\mathbf{Z}_{\circ}	2

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
NOTE						
MAX.	DE	POINTS	2	Note	maximale:	12 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale : 7 points Note		
N° CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée détient une (1) certifications énumérées des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CCSP); and/or Professional (SCCP); and/or Systems Security Certified Professional (SSCP). Une copie des certifications valides de la ressource doit être jointe à la soumission.	Total:		
$\overset{\circ}{\mathbf{Z}}$			C3			

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

\mathbf{N}°	CRITÈRES	BARÈME DE NOTATION	MAX. NOTE	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.8 A	C.8 Analyste de la sécurité des réseaux – Niveau 3	ux – Niveau 3			
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins trois (3) années d'expérience	des solutions de sécurité des TI			
	combinée dans l'examen, l'analyse	énumérées			
	et la mise en œuvre d'au moins	3 points = minimum d'expérience			
	deux (2) des solutions en matière de	combinée démontrée avec trois (3)			
	sécurité des suivantes :	des solutions de sécurité des TI			
		énumérées			
	1) protocoles de sécurité Internet;	4 points = minimum d'expérience			
	2) protocoles réseau;	combinée démontrée avec quatre (4)			
	3) algorithmes cryptographiques;	des solutions de sécurité des TI			
	4) normes d'annuaire;	énumérées			
	5) renforcement de la sécurité	5 points = minimum d'expérience			
	réseau;	combinée démontrée avec cinq (5)			
	6) systèmes d'exploitation.	des solutions de sécurité des TI			
		énumérées			

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PAKAGKAPHE)	
NOTE			
MAX.	DE	FOINTS	۶.
BARÈME DE NOTATION			3 points = minimum d'expérience combinée démontrée dans trois (3) des domaines énumérés 4 points = minimum d'expérience combinée démontrée dans quatre (4) des domaines énumérés 5 points = minimum d'expérience combinée démontrée dans cinq (5) ou plus des domaines énumérés
CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience dans l'élaboration d'exigences et la conception d'applications et d'infrastructures de sécurité des TI dans au moins trois (3) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS); 5) Gestion de l'information et des incidents de sécurité (SIEM); 6) Saisie intégrale de paquet (FPC); 7) Contrôle de l'accès au réseau (NAC); 8) Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou 9) Protection des terminaux.
$\overset{\circ}{\mathbf{Z}}$			2

RÉFÉRENCE À LA	PROPOSITION (PAGE ET PARAGRAPHE)				
NOTE					
MAX. NOTE	POINTS	6	Note	maximale:	12 points
BARÈME DE NOTATION		2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale : 7 points Note		
CRITÈRES		L'entrepreneur doit démontrer que la ressource proposée détient une des certifications suivantes: 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CCSP); and/or Professional (CCSP); and/or 3) Systems Security Certified Professional (SSCP); Une copie des certifications valides de la ressource doit être jointe à la soumission.	Total:		
$\overset{\circ}{\mathbf{Z}}$		C3			

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

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 Pour faciliter l'évaluation des ressources, les entrepreneurs doivent préparer et soumettre leur réponse à un projet d'autorisation de tâches en vitæ. Seule la réponse demandée devrait être fournie.

CRITÈRES OBLIGATOIRES

C.3 Analyste de la certification et Accréditation (C et A) et de l'évaluation de la menace et des risques (EMR) en sécurité des

C.3 Analyste de la C et A et des EMR en sécurité des TI – Niveau 3 Ol L'entrepreneur doit démontrer que la ressource proposée au moins dix (10) années d'expérience combinée acquise au cours des quinze (15) dernières années à la réalisation d'EMR en matière de C et A.		EAIGENCE	RESPECTEE		COMMENTAIRES (ENDROIT DANS LA
M et je je je				RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
M et je					
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 à la réalisation d'EMR en matière de sécurité des TI ou en matière de C et A.	Ü	3 Analyste de la C et A et des EMR e	n sécurité des T	T – Niveau 3	
Uterpreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience combinée acquise au cours des quinze (15) dermières années à la réalisation d'EMR en matière de cet A.					
ressource proposée possède au moins dix (10) années d'expérience combinée acquise au cours des quinze (15) dernières années à la réalisation d'EMR en matière de sécurité des TI ou en matière de C et A.	01	L'entrepreneur doit démontrer que la			
dix (10) années d'expérience combinée acquise au cours des quinze (15) dernières années à la réalisation d'EMR en matière de sécurité des TI ou en matière de C et A.		ressource proposée possède au moins			
acquise au cours des quinze (15) dernières années à la réalisation d'EMR en matière de sécurité des TI ou en matière de C et A.		dix (10) années d'expérience combinée			
années à la réalisation d'EMR en matière de sécurité des TI ou en matière de C et A.		acquise au cours des quinze (15) dernières			
de sécurité des TI ou en matière de C et A.		années à la réalisation d'EMR en matière			
		de sécurité des TI ou en matière de C et A.			

COMMENTAIRES (ENDROIT DANS LA	RESPECTÉE PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)		
NON	RESPECTÉ		
RESPECTÉE			
EXIGENCE		L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience acquise au cours des cinq (5) dernières années dans l'évaluation de l'application de contrôles de sécurité, de l'évaluation des menaces et des risques associés à un système de TI ou de l'interprétation et de l'application des Conseils en matière de sécurité des technologies de l'information 33 (ITSG-33).	Conforme (oui/non)?
		02	

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

COMMENTAIRES (ENDROIT DANS LA ÉE PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)																		
NON RESPECTÉE																		
RESPECTÉE																		
EXIGENCE RESPECTÉE NON RESPECTÉE RESPECTÉE	C.5 Spécialiste de l'ICP – Niveau 3		dans la mise en œuvre et le soutien de solutions d'ICP.	L'entrepreneur doit démontrer que la	ressource proposee possede au moins trois (3) années d'expérience combinée	dans la rédaction d'au moins trois (3) des	types de documents d'ingénierie des systèmes suivants :	 spécifications de la conception 	du système;	 documents sur la conception et la configuration: 	concept d'opération (CONOP);	 plans de mise en œuvre de 	systèmes;	 plans et rapports de mises à 	l'essai;	 plans de soutien du cycle de vie. 	Conforme (oui/non)?	
3	C.5	01		02														

C.6 Ingénieur en sécurité des TI – Niveau 1 U'entrepreneur doit démontrer que la ressource proposée possède au moins une (1) année d'expérience acquise au cours des cinq (5) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS).	RESPECTÉE PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
L'entrepreneur doit démontrer que l'essource proposée possède au moiu une (1) année d'expérience acquise cours des cinq (5) dernières années l'élaboration et la mise en œuvre d'applications et d'infrastructures d sécurité des TI dans au moins un (1 domaines suivants : 1) Systèmes de prévention de intrusions au niveau de l'h (HIPS); 2) Technologies de sécurité d réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention de intrusions dans un réseaut (
L'entrepreneur doit démontrer que l'essource proposée possède au moin une (1) année d'expérience acquise cours des cinq (5) dernières années l'élaboration et la mise en œuvre d'applications et d'infrastructures d sécurité des TI dans au moins un (1 domaines suivants : 1) Systèmes de prévention de intrusions au niveau de l'h (HIPS); 2) Technologies de sécurité d réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention de intrusions dans un réseaut (
L'entrepreneur doit démontrer que l'essource proposée possède au moin une (1) année d'expérience acquise cours des cinq (5) dernières années l'élaboration et la mise en œuvre d'applications et d'infrastructures d sécurité des TI dans au moins un (1 domaines suivants : 1) Systèmes de prévention de intrusions au niveau de l'h (HIPS); 2) Technologies de sécurité d réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention de intrusions dans un réseaut	
L'entreprressource une (1) a cours des l'élabora d'applica sécurité d domaine. 1) 2) 2) 4)	
ressource proposée possède au moins une (1) année d'expérience acquise au cours des cinq (5) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS);	
une (1) année d'expérience acquise au cours des cinq (5) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
cours des cinq (5) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
sécurité des TI dans au moins un (1) des domaines suivants : 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS):	
infriisions dans un réseau (IPS):	
(/a rr) manager to a cross that	
5) Gestion de l'information et des	
incidents de sécurité (SIEM);	
6) Saisie intégrale de paquet	
(FPC);	
7) Contrôle de l'accès au réseau	
(NAC);	
8) Gestion de l'identité, des	
justificatifs d'identité et de	
l'accès (ICAM); et/ou	
9) Protection des terminaux.	

COMMENTAIRES (ENDROIT DANS LA	PROPOSITION, CRITERES NON SATISFAITS, ETC.)																		
NON	RESPECTEE																		
RESPECTÉE																			
EXIGENCE		L'entrepreneur doit démontrer que la	ressource proposée possède au moins	une (1) année d'expérience combinée	dans la rédaction d'au moins deux (2)	des types de documents d'ingénierie des	systèmes suivants:	 spécifications de la conception 	du système;	 documents sur la conception et 	la configuration;	• CONOP;	 plans de mise en œuvre de 	systèmes;	 plans et rapports de mises à 	l'essai;	 plans de soutien du cycle de vie. 	Conforme (oui/non)?	
		02																	

(•	1	
	=	3	
		ţ	
	d	ر >	
	Ę	3	
	_	4	
		l	
Ĺ		7	
	0	3	
	ζ	3	
•	٥	Ņ	
•	ï	3	
	5	֡֡֡֡	
١	Q	2	
	_	-	
	9	j	
	•	=	
		2	
•	ì		
	è	Ú	
	2	Ξ	
		Ľ	
١	£	?	
,		7	

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
			RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C.6	C.6 Ingénieur en sécurité des TI – Nive	Niveau 2		
01				
_	ressource proposée possède au moins			
_	cinq (5) années d'expérience acquise au			
	cours des dix (10) dernières années dans			
_	l'élaboration et la mise en œuvre			
_	d'applications et d'infrastructures de			
_	sécurité des TI dans au moins deux (2)			
-	des domaines suivants :			
	1) Systèmes de prévention des			
_	intrusions au niveau de l'hôte			
_	(HIPS);			
_	2) Technologies de sécurité de			
_	_			
_	3) Systèmes de détection			
_	d'intrusion (IDS);			
_	4) Systèmes de prévention des			
_	intrusions dans un réseau (IPS);			
_	5) Gestion de l'information et des			
_	incidents de sécurité (SIEM);			
_	6) Saisie intégrale de paquet			
_	(FPC);			
_	7) Contrôle de l'accès au réseau			
_	(NAC);			
_	8) Gestion de l'identité, des			
_	justificatifs d'identité et de			
_	l'accès (ICAM); et/ou			
_	9) Protection des terminaux.			

EXIGENCE RESPECTÉE O2 L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception et la configuration; • convop: • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de soutien du cycle de vie. Conforme (oui/non)?	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)		
EXIGENCE L'entrepreneur doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de soutien du cycle de vie. Conforme (oui/non)?	NON RESPECTÉE		
EXIGE L'entrep ressource deux (2) dans la r das type systèmee • • • Confort	RESPECTÉE		
00	EXIGENCE	L'entrep ressourc deux (2) dans la r des types systèmes	Conforme (oui/non)?

		Tannadada	NON	A 1 SIM A THOUGHAND SERLY ATMENTAL MANOR
	EAIGENCE	KESFECIEE	DECPECTÉE	PROPOSITION CRITERIES NON SATISFAIRS FITS
				INUFUSITION, CRITENES NON SALISFALIS, ELC.)
Ü	C.6 Ingénieur en sécurité des TI – Niveau 3	8m 3		
01				
	ressource proposée possède au moins			
	dix (10) années d'expérience acquise au			
	cours des quinze (15) dernières années			
	dans l'élaboration et la mise en œuvre			
	d'applications et d'infrastructures de			
	sécurité des TI dans au moins deux (2)			
	des domaines suivants :			
	1) Systèmes de prévention des			
	intrusions au niveau de l'hôte			
	(HIPS);			
	2) Technologies de sécurité de			
	réseautage sans fil;			
	3) Systèmes de détection			
	d'intrusion (IDS);			
	4) Systèmes de prévention des			
	intrusions dans un réseau (IPS);			
	5) Gestion de l'information et des			
	incidents de sécurité (SIEM);			
	6) Saisie intégrale de paquet			
	7) Contrôle de l'accès au réseau			
	(NAC);			
	8) Gestion de l'identité, des			
	justificatifs d'identité et de			
	l'accès (ICAM); et/ou			
	9) Protection des terminaux.			

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA
			RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
Ö	O2 L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	trois (3) années d'expérience combinée			
	dans la rédaction d'au moins trois (3) des			
	types de documents d'ingénierie des			
	systèmes suivants:			
	 spécifications de la conception 			
	du système;			
	documents sur la conception et			
	la configuration;			
	• CONOP;			
	• plans de mise en œuvre de			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	Conforme (oui/non)?			

<u>:</u>	C./ Specialiste en conception de securite des 11 – Iviveau 3	e des 11 – Mive	au J	
	EXIGENCE	RESPECTÉE		COMMENTAIRES (ENDROIT DANS LA
			RESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
S	C.7 Snécialiste en concention de sécurité des TI – Niveau 3	ité des TI – Niv	ean 3	
)				
01	1 L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	dix (10) années d'expérience acquise au			
	cours des quinze (15) dernières années			
	dans la planification et la mise en œuvre			
	d'architectures d'intégration de la			
	sécurité des TI.			
02	L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	trois (3) années d'expérience combinée			
	dans la rédaction d'au moins trois (3) des			
	types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception 			
	du système;			
	 documents sur la conception et 			
	la configuration;			
	• CONOP;			
	 plans de mise en œuvre de 			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	• plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

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

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION CULTÈDES NON SATISEATTS ETC.)
			NESFECIEE	FROFOSITION, CRITENES NON SATISFAILS, ETC.)
C.	C.8 Analyste de la sécurité des réseaux – Niveau 3	x – Niveau 3		
10	L'entrepreneur doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes: 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.			

C.9 Opérat O1 L'entrep ressourc dix (10) cours de dans l'es cuvre or des techn	C.9 Opérateur de systèmes de sécurité 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 dans l'examen, l'analyse, la mise en	rité des TI – Niveau 3	ESPECTÉE	PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
	preneur de systèmes de sécurité preneur doit démontrer que la ce proposée possède au moins années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en	les TI – Niveau	6	
	treur de systèmes de sécurité preneur doit démontrer que la ce proposée possède au moins années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en	les TI – Niveau	9	
	preneur doit démontrer que la ce proposée possède au moins) années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en			
	preneur doit démontrer que la ce proposée possède au moins) années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en			
ressourc dix (10) cours de dans l'es œuvre or des tech	ce proposée possède au moins) années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en			
dix (10) cours de dans l'ex œuvre or des tech	o) années d'expérience acquise au les quinze (15) dernières années examen, l'analyse, la mise en			
cours de dans l'ex œuvre or des tech l	les quinze (15) dernières années examen, l'analyse, la mise en			
dans l'es œuvre or des tech	examen, l'analyse, la mise en			
des techi				
des techi	œuvre ou le soutien d'au moins deux (2)			
1) pr	des technologies suivantes :			
1) pr				
	1) protocoles de sécurité Internet;			
2) pr	2) protocoles réseau;			
3) al	3) algorithmes cryptographiques;			
4) no	4) normes d'annuaire;			
5) re	5) renforcement de la sécurité réseau;			
(9 sy	systèmes d'exploitation.			

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

֡֡֞֞֞֓֞֞֞֞֡֞֞֓֞֡֞֞֞֓֞֞֞֞֞֓֓֡֡֡֡֡֡֡֡֡	ili alialyses de vull		
	EXIGENCE		
		RESPECTEE PROPOSITION, CRITERES NON SATISFAITS, ETC.)	AITS, ETC.)
ن ت	C.11 Spécialiste en analyses de vulnérabilité de la sécurité des TI – Niveau 3	llité de la sécurité des TI – Niveau 3	
01	L'entrepreneur doit démontrer que la rescource proposée possède au moins		
	dix (10) années d'expérience acquise au		
	cours des quinze (15) dernières années		
	dans la realisation d'analyses de la vulnérabilité de la sécurité des TI.		
02	L'entrepreneur doit démontrer que la		
	ressource proposée possède au moins		
	cinq (5) années d'expérience acquise au		
	cours des dix (10) dermères années dans		
	l'administration et l'évaluation d'outils		
	d'analyse des agents de menace et des		
	technologies émergentes dans au moins		
	un (1) des domaines suivants :		
	1) protection des renseignements		
	personnels, analyse predictive,		
	VolP, visualisation et fusion des		
	2) dispositifs de sécurité sans fil,		
	3) détecteurs d'accès entrant et		
	4) services consultatifs publics en		
	matière de vulnérabilité des TI;		
	5) analyseurs de réseau et outils		
	d'analyse des vulnérabilités		
	comme le logiciel SATAN		
	(Security Administrator Tool for		
	Analysing Networks), le soutien en		
	service (ISS), Portscan, KALI et		
	NMap.		
		_	

EXIGENCE	RESPECTÉE	NON RESPECTÉE	NON COMMENTAIRES (ENDROIT DANS LA SPECTÉE PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
Conforme (oui/non)?			

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

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
ز	C.12 Spécialiste de la gestion des incidents – Niveau 3	ents – Niveau 3		
01	L'entrepreneur doit démontrer que la ressource proposée possède au moins			
	dix (10) années d'expérience acquise au cours des quinze (15) dernières années			
	dans la gestion des incidents de sécurité des TI.			
02	L'entrepreneur doit démontrer que la			
	ressource proposée possède au moins			
	cinq (5) années d'expérience acquise au			
	assurer le soutien d'au moins une (1) des			
	analyses des incidents suivantes :			
	1) mécanismes d'intervention;			
	2) plans de prévention et			
	d'intervention d'urgence;			
	3) activités du Centre des opérations			
	d'urgence.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

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

IE RÉFÉRENCE À LA PROPOSITION (PAGE ET	PARAGRAPHE)		
MAX. NOTE DE	POINTS	4	4
N° CRITÈRES BARÈME DE NOTATION	TR en sécurité des TI – Niveau 3	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience
N° CRITÈRES	C.3 Analyste de la C et A et des EM	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience de la réalisation de tâches en sécurité des TI conformément à la Politique du gouvernement sur la sécurité et aux documents connexes de toute combinaison avec au moins un (1) organisme responsable ciaprès: 1) Gendarmerie royale du Canada; 2) Centre de la sécurité des télécommunications; 3) Secrétariat du Conseil du Trésor du Canada.	L'entrepreneur doit démontrer que la ressource proposée possède l'expérience de l'analyse de la conception d'architectures de sécurité des TI.
$^{\circ}$ Z	C.3 A	C1	C3

\mathbf{z}°	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			POINTS		PROPOSITION (PAGE ET PARAGRAPHE)
C 4	L'entrepreneur doit démontrer que la ressource proposée a suivi l'un (1) des cours de formation suivants :	2 points = preuve d'au moins une des certifications énumérées	7		
	administrateur certifié de RSA Archer; administrateur d'OpenPages d'IBM;				
	3) administrateur certifié en gestion d'administration de système de gouvernance, risque et conformité de Metricstream.				
	Une copie du certificat de cours valide de la ressource proposée doit être jointe à la soumission.				
C2	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience de la production et de l'évaluation de produits livrables de C et A aux fins d'accréditation d'un système de 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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
	Total:	Note de passage minimale : 11 points	Note maximale: 18 points		

21/45

C.5 Spécialiste de l'ICP – Niveau 3	
pécialiste de l'ICP – Niveau	m
pécialiste de l'ICP –	ean
pécialiste de l'ICP –	Ż
C.5 Spécialiste de l'ICP	- 1
C.5 Spécialiste de l'I	CP
C.5 Spécialiste de	ľ
C.5 Spécialiste	de
C.5 Spéciali	ste
C.5 Spéci	ali
C.5 Sp	<u>ě</u>
C.5	S
	C.5

RÉFÉRENCE À LA PROPOSITION (PAGE ET	PARAGRAPHE)																												
NOTE																													
MAX.	POINT S		5																										
BARÈME DE NOTATION			1 point = minimum d'expérience	combinée démontrée avec une (1)	des technologies énoncées dans un	contexte d'ICP	2 points = minimum d'expérience	combinée démontrée avec deux (2)	des technologies énoncées dans un	contexte d'ICP	3 points = minimum d'expérience	combinée démontrée avec trois (3)	des technologies énoncées dans un	contexte d'ICP	4 points = minimum d'expérience	combinée démontrée avec quatre (4)	des technologies énoncées dans un	contexte d'ICP	5 points = minimum d'expérience	combinée démontrée avec au moins	cinq (5) des technologies énoncées	dans un contexte d'ICP							
N° CRITÈRES		C.5 Spécialiste de l'ICP – Niveau 3	L'entrepreneur doit démontrer que	la ressource proposée possède au	moins cinq (5) années	d'expérience combinée dans	l'examen, l'analyse, la mise en	œuvre et le soutien des	technologies suivantes dans un	contexte d'ICP:		1) architectures d'ICP;	2) signatures numériques et	chiffrement;	3) produits d'ICP, notamment	l'autorité de certification et	l'autorité d'enregistrement;	4) produits reposant sur des	clés publiques, comme les	réseaux privés virtuels, la	voix par le protocole Internet	et l'extension S/MIME;	5) produits d'annuaire X.500;	6) normes de certificat X.509;	7) protocoles de sécurité	Internet;	8) produits du protocole de	vérification en ligne de l'état	des certificats.
$\overset{\circ}{\mathbf{Z}}$		C.5 S ₁	C1																										

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)		
NOTE		
MAX. DE POINT S	4	4
BARÈME DE NOTATION	I point = de 1 à 3 années d'expérience 2 points = plus de 3 à 5 années d'expérience 3 points = plus de 5 à 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience combinée dans les éléments suivants: 1) élaboration de politiques de certification pour l'ICP; 2) élaboration d'énoncés de pratiques de certification pour l'ICP; 3) vérifications et inspections de la conformité à la politique de certification pour l'ICP.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience combinée dans la rédaction des documents d'ingénierie suivants liés à l'ICP: 1) architectures de solutions; 2) analyse d'options; 3) mesures de rendement des systèmes et de la planification de la capacité; 4) plans de continuité des activités et de reprise après sinistre.
$\overset{\circ}{\mathbf{Z}}$	C2	C3

REFERENCE A LA PROPOSITION (PAGE ET PARAGRAPHE)	
NOTE	
MAX. DE POINT S	'n
BAREME DE NOTATION	I point = minimum d'expérience combinée démontrée avec un (1) des produits/solutions d'ICP énumérés 2 points = minimum d'expérience combinée démontrée avec deux (2) des produits/solutions d'ICP énumérés 3 points = minimum d'expérience combinée démontrée avec trois (3) des produits/solutions d'ICP énumérés 4 points = minimum d'expérience combinée démontrée avec quatre (4) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec quatre (4) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec au moins cinq (5) des produits/solutions d'ICP énumérés
CRITERES	L'entrepreneur doit démontrer que la ressource proposée a travaillé pendant au moins cinq (5) années avec les produits/solutions d'ICP ci-dessous: 1) autorité de certification Entrust; 2) autorité de certification Microsoft; 3) modules de sécurité matérielle; 4) solutions de gestion des cartes; 5) cartes à puce et logiciels des cartes à puce; 6) logiciel client Entrust.
0	C4

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE POINT		PROPOSITION (PAGE ET PARAGRAPHE)
			S		
S	L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications suivantes :	2 points = preuve d'au moins une des certifications énumérées	2		
	1) Certified Information				
	System Security				
	2) Certified Cloud Security				
	Professional (CCSP);				
	3) Systems Security Corrified Professional				
	(SSCP).				
	Une copie des certifications				
	valides de la ressource proposée doit être jointe à la soumission.				
	Total:	Note de passage minimale :	Note		
		12 points	maximale		
			20 points		

C.6 Ingénieur en sécurité des TI – Niveau 1

	carity act it	Ivenu I			
$\overset{\circ}{\mathbf{Z}}$	N° CRITERES	BAREME DE NOTATION	MAX.	NOTE	REFERENCE A LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6 I	Ingénieur en sécurité des TI – N	Viveau 1			
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	9		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins une (1) année d'expérience	des solutions de sécurité des TI			
	combinée de l'élaboration et de la	énumérées			
	documentation de spécifications	3 points = minimum d'expérience			
	relatives aux exigences de système	combinée démontrée avec trois (3)			
	pour au moins deux (2) des	des solutions de sécurité des TI			
	solutions en matière de sécurité des	énumérées			
	TI suivantes:	4 points = minimum d'expérience			
		combinée démontrée avec quatre (4)			
	1) Systèmes de prévention des	des solutions de sécurité des TI			
	intrusions au niveau de	énumérées			
	l'hôte (HIPS);	5 points = minimum d'expérience			
	2) Technologies de sécurité	combinée démontrée avec cinq (5) des			
	de réseautage sans fil;	solutions de sécurité des TI			
	3) Systèmes de détection	énumérées			
	d'intrusion (IDS);	6 points = minimum d'expérience			
	4) Systèmes de prévention des	combinée démontrée avec au moins			
	intrusions dans un réseau	six (6) des solutions de sécurité des TI			
	(IPS);	énumérées			
	5) Gestion de l'information et				
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	9) Protection des terminaux				

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)				
NOTE				
MAX. DE POINTS	3	3	3	Note maximale: 15 points
BARÈME DE NOTATION	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	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	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	Note de passage minimale : 8 points Note maxi
CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.	Total:
$\overset{\circ}{\mathbf{Z}}$	72	ව	C4	

C.6 Ingénieur en sécurité des TI – Niveau 2

1.0 1	C.0 Ingenieur en securite des 11 – Miveau 2	veau z			
$\overset{\circ}{\mathbf{Z}}$	CRITERES	BAREME DE NOTATION	MAX.	NOTE	REFERENCE A LA
			DE POINTS		PROPOSITION (PAGE ET PARAGRAPHE)
C.6 I	C.6 Ingénieur en sécurité des TI – Ni	Niveau 2			
C1	L'entrepreneur doit démontrer que	1 point = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec une (1) des			
	moins deux (2) années d'expérience	solutions de sécurité des TI			
	combinée de l'élaboration et de la	énumérées			
	documentation de spécifications	2 points = minimum d'expérience			
	relatives aux exigences de système	combinée démontrée avec deux (2)			
	pour les solutions en matière de	des solutions de sécurité des TI			
	sécurité des TI suivantes :	énumérées			
		3 points = minimum d'expérience			
	1) Systèmes de prévention des	combinée démontrée avec trois (3)			
	intrusions au niveau de	des solutions de sécurité des TI			
	l'hôte (HIPS);	énumérées			
	2) Technologies de sécurité	4 points = minimum d'expérience			
	de réseautage sans fil;	combinée démontrée avec quatre (4)			
	3) Systèmes de détection	des solutions de sécurité des TI			
	d'intrusion (IDS);	énumérées			
	4) Systèmes de prévention des	5 points = minimum d'expérience			
	intrusions dans un réseau	combinée démontrée avec au moins			
	(IPS);	cinq (5) des solutions de sécurité des			
	5) Gestion de l'information et	TI énumérées			
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	9) Protection des terminaux				

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)			
NOTE			
MAX. DE POINTS	4	4	4
BARÈME DE NOTATION	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	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	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
N° CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.
$\overset{\circ}{\mathbf{Z}}$	C2	C3	C4

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
NOTE						
MAX.	DE	POINTS	2	Note	maximale:	19 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale :	11 points	
N° CRITÈRES			preneur doit démontrer que uurce proposée détient une (1) tifications suivantes : ertified Information System ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être la soumission.	Total:		
$\overset{\circ}{\mathbf{Z}}$			CS			

C.6 Ingénieur en sécurité des TI – Niveau 3

		Ivcau 3			, ,
\mathbf{z}	CRITERES	BAREME DE NOTATION	MAX.	NOTE	REFERENCE A LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6	C.6 Ingénieur en sécurité des TI – Ni	Viveau 3			
C1	L'entrepreneur doit démontrer que	1 point = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec une (1) des			
	moins quatre (4) années	solutions de sécurité des TI			
	d'expérience combinée de	énumérées			
	l'élaboration et de la documentation	2 points = minimum d'expérience			
	de spécifications relatives aux	combinée démontrée avec deux (2)			
	exigences de système pour les	des solutions de sécurité des TI			
	solutions en matière de sécurité des	énumérées			
	TI suivantes:	3 points = minimum d'expérience			
		combinée démontrée avec trois (3)			
	1) Systèmes de prévention des	des solutions de sécurité des TI			
	intrusions au niveau de	énumérées			
	l'hôte (HIPS);	4 points = minimum d'expérience			
	2) Technologies de sécurité	combinée démontrée avec quatre (4)			
	de réseautage sans fil;	des solutions de sécurité des TI			
	3) Systèmes de détection	énumérées			
	d'intrusion (IDS);	5 points = minimum d'expérience			
	4) Systèmes de prévention des	combinée démontrée avec au moins			
	intrusions dans un réseau	cinq (5) des solutions de sécurité des			
		TI énumérées			
	5) Gestion de l'information et				
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	9) Protection des terminaux				

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)			
NOTE			
MAX. DE POINTS	4	4	4
BARÈME DE NOTATION	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 8 années d'expérience. 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience. 4 points = plus de 8 années d'expérience
N° CRITÈRES	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.
$\overset{\circ}{\mathbf{Z}}$	C2	C3	C4

$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PAKAGKAPHE)
\mathcal{S}	L'entrepreneur doit démontrer que la ressource détient une (1) des certifications suivantes:	2 points = preuve d'au moins une des certifications énumérées	2		
	Certified Information System Security Professional (CISSD).				
	2) Certified Cloud Security				
	3) Systems Security Certified				
	Professional (SSCP).				
	Une copie des certifications valides				
	de la ressource proposée doit être jointe à la soumission.				
	Total:	Note de passage minimale :	Note		
		11 points	maximale:		
			ट्यागाव दा		

C.7 Spécialiste en conception de sécurité des TI – Niveau 3

°Z	N° CRITTÈRES BARÈME DE NOTA	RABEME DE NOTATION	MAX	ATON	PÉFÉPENCE À LA
-			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.7 S	Spécialiste en conception de séc	urité des TI – Niveau 3			
Ü	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans la conception d'architectures sécurisées en respectant les lignes directrices des conseils en matière de sécurité des technologies de l'information du Centre de la sécurité des télécommunications.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C3	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans l'analyse d'au moins un (1) des éléments suivants: 1) outils et techniques de sécurité des TI; 2) données de sécurité et présentation d'avis et de rapports; 3) statistiques sur la sécurité des 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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
ខ	L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience dans les études de classification ou de désignation du niveau de sécurité des données.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)			
NOTE					
MAX.	DE	POINTS	Note	maximale:	20 points
BARÈME DE NOTATION MAX.			Note de passage minimale :	12 points	
CRITÈRES			Total:		
$\overset{\circ}{\mathbf{Z}}$					

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

\mathbf{N}_{\circ}	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.8 A	C.8 Analyste de la sécurité des réseaux – Niveau 3	ux – Niveau 3			
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	5		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins trois (3) années d'expérience	des solutions de sécurité des TI			
	combinée dans l'examen, l'analyse,	énumérées			
	la mise en œuvre et l'appui d'au	3 points = minimum d'expérience			
	moins deux (2) des solutions en	combinée démontrée avec trois (3)			
	matière de sécurité suivantes :	des solutions de sécurité des TI			
		énumérées			
	1) protocoles de sécurité Internet;	4 points = minimum d'expérience			
	2) protocoles réseau;	combinée démontrée avec			
	3) algorithmes cryptographiques;	quatre (4) des solutions de sécurité			
	4) normes d'annuaire;	des TI énumérées			
	5) renforcement de la sécurité	5 points = minimum d'expérience			
	réseau;	combinée démontrée avec cinq (5)			
	6) systèmes d'exploitation.	des solutions de sécurité des TI			
		énumérées			

	PROPOSITION (PAGE ET	PARAGRAPHE)																													
NOTE																															
MAX.	DE	POINTS	5																												
BARÈME DE NOTATION			3 points = minimum d'expérience	combinee demondee dans dots (3)	des domaines enumeres	4 points = minimum d'expérience	combinée démontrée dans	quatre (4) des domaines énumérés	5 points = minimum d'expérience	combinée démontrée dans cinq (5) ou plus des domaines énumérés	•																				
CRITÈRES			L'entrepreneur doit démontrer que	ra ressource proposee posseue au	moins deux (2) annees d'experience	dans l'élaboration d'exigences et la	conception d'applications et	d'infrastructures de sécurité des TI	dans au moins trois (3) des	domaines suivants:	1) Systèmes de prévention des	intrusions au niveau de	l'hôte (HIPS);	2) Technologies de sécurité	de réseautage sans fil;	3) Systèmes de détection	d'intrusion (IDS);	4) Systèmes de prévention des	intrusions dans un réseau	(IPS);	5) Gestion de l'information et	des incidents de sécurité	(SIEM);	6) Saisie intégrale de paquet	(FPC);	7) Contrôle de l'accès au	réseau (NAC);	8) Gestion de l'identité, des	justificatifs d'identité et de	l'accès (ICAM); et/ou	9) Protection des terminaux
$\overset{\circ}{\mathbf{Z}}$			C2																												

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
NOTE						
MAX.	DE	POINTS	2	Note	maximale:	12 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale :	7 points	
N° CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications suivantes: 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CCSP); 2) Certified Cloud Security Professional (CCSP); 3) Systems Security Certified Professional (SSCP). Une copie des certifications valides de la ressource proposée doit être jointe à la soumission.			
$\overset{\circ}{\mathbf{Z}}$			S			

C.9 Opérateur de systèmes de sécurité des TI – Niveau 3

; ;	ystemes de secui	ite ues 11 – Miveau 3			
$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.9	9 Opérateur de systèmes de sécuri	rité des TI – Niveau 3			
CI	L'entrepreneur doit démontrer que	3 points = minimum d'expérience	9		
	la ressource proposée possède au	combinée démontrée avec trois (3)			
	moins deux (2) années d'expérience	des solutions de sécurité des TI			
	combinée dans l'examen, l'analyse,	énumérées			
	la mise en œuvre ou l'appui d'au	4 points = minimum d'expérience			
	moins trois (3) des solutions ou plus	combinée démontrée avec			
	en matière de sécurité des TI	quatre (4) des solutions de sécurité			
	suivantes:	des TI énumérées			
		5 points = minimum d'expérience			
	1) Systèmes de prévention des	combinée démontrée avec cinq (5)			
	intrusions au niveau de	des solutions de sécurité des TI			
	l'hôte (HIPS);	énumérées			
	2) Technologies de sécurité	6 points = minimum d'expérience			
	de réseautage sans fil;	combinée démontrée avec au moins			
	3) Systèmes de détection	six (6) des solutions de sécurité des			
	d'intrusion (IDS);	TI énumérées			
	4) Systèmes de prévention des				
	intrusions dans un réseau				
	(IPS);				
	5) Gestion de l'information et				
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	9) Protection des terminaux				

C2 L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications énumérées des certifications suivantes: 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CISSP); 3) Systems Security Certified Professional (SISP). 4) Une copie des certifications valides de la ressource proposée doit être jointe à la soumission. Note de passage minimale : Repoints la project de la resource proposée doit être jointe à la soumission. Note de passage minimale : Repoints la points la pointe la la commission.	$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications énumérées des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CSSP); and/or 3) Systems Security Certified Professional (SSCP). Une copie des certifications valides de la ressource proposée doit être jointe à la soumission. Note de passage minimale : Spoints Polity Professional (SSCP) Polity Profe				DE		PROPOSITION (PAGE ET
L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications énumérées des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CSSP); 3) Systems Security Certified Professional (SSCP). Une copie des certifications valides de la ressource proposée doit être jointe à la soumission. Total: Spoints = preuve d'au moins une des certifications valides des certifications valides de la ressource proposée doit être jointe à la soumission.				POINTS		PARAGRAPHE)
ertified Information System ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or systems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être i.la soumission. Note de passage minimale: 5 points	C2	L'entrepreneur doit démontrer que	2 points = preuve d'au moins une	2		
ertified Information System ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or systems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale: 5 points		la ressource proposée détient une (1)	des certifications énumérées			
ertified Information System ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être . la soumission. Note de passage minimale: 5 points		des certifications survantes :				
erutined Information System ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être . Ia soumission. Note de passage minimale: 5 points		· · · · · · · · · · · · · · · · · · ·				
ecurity Professional (CISSP); ertified Cloud Security rofessional (CCSP); and/or ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être . la soumission. Note de passage minimale: 5 points		1) Certified Information System				
ertified Cloud Security rofessional (CCSP); and/or ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale: 5 points		Security Professional (CISSP);				
rofessional (CCSP); and/or systems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale: 5 points		2) Certified Cloud Security				
ystems Security Certified rofessional (SSCP). pie des certifications valides ssource proposée doit être La soumission. Note de passage minimale: 5 points		Professional (CCSP); and/or				
rofessional (SSCP). pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale: 5 points		3) Systems Security Certified				
pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale : 5 points		Professional (SSCP).				
pie des certifications valides ssource proposée doit être la soumission. Note de passage minimale : 5 points						
ssource proposée doit être la soumission. Note de passage minimale: 5 points		Une copie des certifications valides				
Note de passage minimale : 5 points		de la ressource proposée doit être				
Note de passage minimale : 5 points		jointe à la soumission.				
			Note de passage minimale :	Note		
8 points			5 points	maximale:		
				8 points		

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

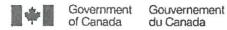
$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.11	C.11 Spécialiste en analyses de vulné	nérabilité de la sécurité des TI – Niveau 3	- Niveau 3		
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	9		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins cinq (5) années d'expérience	des technologies énumérées			
	combinée dans l'examen, l'analyse	3 points = minimum d'expérience			
	et le soutien d'au moins deux (2)	combinée démontrée avec trois (3)			
	des technologies suivantes :	des technologies énumérées			
		4 points = minimum d'expérience			
	rité Internet;	combinée démontrée avec			
	2) protocoles réseau;	quatre (4) des technologies			
	3) réseau sans fil;	énumérées			
	4) normes d'annuaire;	5 points = minimum d'expérience			
	5) renforcement de la sécurité	combinée démontrée avec cinq (5)			
	réseau;	des technologies énumérées			
	6) systèmes d'exploitation.	6 points = minimum d'expérience			
		combinée démontrée avec six (6)			
		des technologies énumérées			

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)			
NOTE					
MAX.	DE	POINTS	4	2	Note maximale: 18 points
BARÈME DE NOTATION			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 8 années d'expérience 4 points = plus de 8 années d'expérience	2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale : 11 points
CRITÈRES			L'entrepreneur doit démontrer que la ressource proposée possède de l'expérience de la documentation et de la fourniture d'information sur les menaces, les vulnérabilités ou les risques liés à la sécurité des TI.	L'entrepreneur doit démontrer que la ressource proposée détient une (1) des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CCSP); and/or 3) Systems Security Certified Professional (SSCP). Une copie des certifications valides de la ressource proposée doit être jointe à la soumission.	Total:
\mathbf{N}°			C3	C4	

C.12 Spécialiste de la gestion des incidents, niveau 3

°Z	N° CRITÈRES	BARFME DE NOTATION	MAX	ATON	RÉFÉRENCE À LA
7		MANAGE DE NOTATION			
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.11	Spécialiste de la gestion des inc	sidents – Niveau 3			
C1	L'entrepreneur doit démontrer que	2 points = minimum d'expérience	S		
	la ressource proposée possède au	combinée démontrée avec deux (2)			
	moins trois (3) années d'expérience	des technologies énumérées			
	combinée dans l'examen, l'analyse	3 points = minimum d'expérience			
	et le soutien d'au moins deux (2)	combinée démontrée avec trois (3)			
	des technologies suivantes :	des technologies énumérées			
	,	4 points = minimum d'expérience			
	1) protocoles de sécurité Internet;	combinée démontrée avec			
	2) protocoles réseau;	quatre (4) des technologies			
	3) normes d'annuaire;	énumérées			
	4) renforcement de la sécurité	5 points = minimum d'expérience			
	réseau;	combinée démontrée avec cinq (5)			
	5) systèmes d'exploitation.	des technologies énumérées			
C7	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années	4		
	la ressource proposée possède de	d'expérience			
	l'expérience de l'utilisation	2 points = plus de 3 à 5 années			
	d'analyseurs de réseau et d'outils	d'expérience			
	d'analyse de la vulnérabilité.	3 points = plus de 5 à 8 années			
		d'expérience			
		4 points = plus de 8 années			
C3	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années	4		
	la ressource proposée possède de	d'expérience			
	l'expérience de la documentation et	2 points = plus de 3 à 5 années			
	de la fourniture d'information sur	d'expérience			
	les menaces, les vulnérabilités ou	3 points = plus de 5 à 8 années			
	les risques liés à la sécurité des TI.	d'expérience			
		4 points = plus de 8 années			
		n experience			

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C4	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années	4		
	la ressource proposée possède de	d'expérience			
	l'expérience de l'analyse des	2 points = plus de 3 à 5 années			
	rapports d'activité, des registres des	d'expérience			
	activités et des incidents relatifs aux	3 points = plus de 5 à 8 années			
	systèmes de TI.	d'expérience			
		4 points = plus de 8 années			
		d'expérience			
C2	L'entrepreneur doit démontrer que	1 point = de 1 à 3 années	4		
	la ressource proposée possède de	d'expérience			
	l'expérience dans un centre de	2 points = plus de 3 à 5 années			
	réponse aux incidents.	d'expérience			
		3 points = plus de 5 à 8 années			
		d'expérience			
		4 points = plus de 8 années			
		d'expérience			
	Total:	Note de passage minimale :	Note		
		13 points	maximale:		
			21 points		



Contract Number /	Numéro du	contrat
		588

W6369-17-P5LA S1 Amendment 1
Security Classification / Classification de sécurité
UNCLASSIFIED

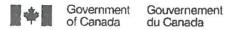
SECURITY REQUIREMENTS CHECK LIST (SRCL)

	CATION DES EXIGENCES RE		ECURITE (LVERS)	
PART A - CONTRACT INFORMATION / PARTIE A 1. Originating Government Department or Organization			or Directorate / Direction génér	ala au Direction
Ministère ou organisme gouvernemental d'origine	DND		SP / DIMEI	ale ou Direction
3. a) Subcontract Number / Numéro du contrat de so			ntractor / Nom et adresse du so	vis-traitant
4. Brief Description of Work / Breve description du tra				
Professional services using the Task-Based Informatics	Professional Services (TBIPS) supply a	rrangement on an as-re	equired basis.	
9 6				
F				
a) Will the supplier require access to Controlled Grant Le fournisseur aura-t-il accès à des marchandis				No V Yes Oui
5. b) Will the supplier require access to unclassified r	military technical data subject to the	provisions of the Te	echnical Data Control	No Yes
Regulations?				Non ✓ Oul
Le fournisseur aura-t-il accès à des données ter sur le contrôle des données techniques?	chniques militaires non classifiées	qui sont assujetties a	aux dispositions du Règlement	
Indicate the type of access required / Indiquer le type	vne d'accès requis			
	•			
 a) Will the supplier and its employees require acce Le fournisseur ainsi que les employés auront-ils 				No / Yes
(Specify the level of access using the chart in Q	acces a des renseignements ou a	des biens PROTEG	ES evou CLASSIFIES?	Non ▼ Oui
(Préciser le niveau d'accès en utilisant le tablea	u qui se trouve à la question 7. c)			
6. b) Will the supplier and its employees (e.g. cleaner	rs, maintenance personnel) require	access to restricted	access areas? No access to	No Yes
PROTECTED and/or CLASSIFIED information (or assets is permitted.			Non Oui
Le foumisseur et ses employés (p. ex. nettoyeu à des renseignements ou à des blens PROTÉG	rs, personnel d'entretien) auront-ils	accès à des zones	d'accès restreintes? L'accès	
6. c) Is this a commercial courier or delivery requirem	est with no everyight storage?	utonse.		No Yes
S'agit-il d'un contrat de messagerie ou de livrais		e de nuit?		Non Oui
7. a) Indicate the type of information that the supplier	will be required to access / Indian	ar la luna d'informatio	on augual la fournireaux daves	
		7		avoir acces
Canada ✓	NATO/OTAN 🗸		Foreign / Étranger	
7. b) Release restrictions / Restrictions relatives à la				
No release restrictions Aucune restriction relative	All NATO countries	7	No release restrictions	
à la diffusion	Tous les pays de l'OTAN	_	Aucune restriction relative à la diffusion	
			a la diridolori	
Not releasable				
A ne pas diffuser				
Restricted to: / Limité à :	Restricted to: / Limité à :	CM .	Restricted to: / Limité à :	
Lemma		J co.		
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le	e(s) pays :	Specify country(ies): / Précise	er le(s) pays :
Canada and United States	CANJUS			
	CAPIOS			
7. c) Level of information / Niveau d'information				
PROTECTED A	NATO UNCLASSIFIED		PROTECTED A	
PROTÈGÉ A	NATO NON CLASSIFIÉ		PROTÉGÉ A	
PROTECTED B	NATO RESTRICTED		PROTECTED B	
PROTECTED C	NATO DIFFUSION RESTREINT NATO CONFIDENTIAL		PROTÉGÉ B PROTECTED C	
PROTÉGÉ C	NATO CONFIDENTIAL		PROTÉGÉ C	
CONFIDENTIAL	NATO SECRET		CONFIDENTIAL	
CONFIDENTIEL	NATO SECRET	1	CONFIDENTIEL	
SECRET	COSMIC TOP SECRET		SECRET	
SECRÉT V	COSMIC TRÈS SECRET		SECRET	
TOP SECRET			TOP SECRET	
TRÈS SECRET			TRÈS SECRET	
TOP SECRET (SIGINT)			TOP SECRET (SIGINT)	
TRÈS SECRET (SIGINT)			TRÈS SECRET (SIGINT)	

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité UNCLASSIFIED

Canadä^{*}



Contract Number / Numéro du contrat W6369-17-P5LA S1

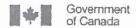
Security Classification / Classification de sécurité UNCLASSIFIED

8 Will the supplier require access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to PROTECTED and/or CLASSIFIED COMPECTATION and the supplier required access to the suppli
8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
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? Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? No Non Oui
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
AAN /
RELIABILITY STATUS CONFIDENTIAL SECRET TOP SECRET TRÈS SECRET
TOP SECRET – SIGINT NATO CONFIDENTIAL NATO SECRET COSMIC TOP SECRET NATO SECRET NATO SECRET COSMIC TRÈS SECRET
SITE ACCESS ACCES 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.
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No Non Ves Oui
If Yes, will unscreened personnel be escorted?
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 Yes
premises?
premises? Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?
premises? Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou
premises? 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? Le fournisseur sera-t-il tenu de protéger des renseignements ou des blens COMSEC? No Yes Couriles au l'entreposer sur place des renseignements ou des blens PROTÉGÉS et/ou
premises? 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?
premises? 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? 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
premises? 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? Le fournisseur sera-t-il tenu de protèger 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?
premises? 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? 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
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériet PROTÉGÉ et/ou CLASSIFIÉ?
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériet PROTÉGÉ
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériet 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 Y Non Oui Yes
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ 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 Non Oui
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériet PROTÉGÉ 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 No Yes No Yes
PRODUCTION 11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIÉS? No
premises? 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? 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? Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériet PROTÉGÉ 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? Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité UNCLASSIFIED

Canadä



Gouvernement du Canada

Contract Number / Numéro du contrat

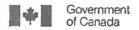
W6369-17-P5LA S1

Security Classification / Classification de sécurité UNCLASSIFIED

PART C - (continue For users comple site(s) or premise Les utilisateurs q niveaux de sauve For users comple Dans le cas des d dans le tableau re	eting es. jui re egar eting utilis	the employed rde r the sate	form lisser equi: form urs q	n manually us nt le formulair s aux installati s online (via ti	e manuell ons du foi ne interne te formuli	lement do urnisseur. I), the sur aire en Ilg	nmary chart nmary chart nne (par Inter	le tableau réc	capitulatif ly populai nses aux	ci-dessou ted by you questions	s pou	ir ind	lique	r, pour chaque	e catégor	ie, les
Category Catégorie		OTECT			ASSIFIED LASSIFIÉ			NATO						COMSEC		
	А	8	С	CONFIDENTIAL	SECRET	TOP	NATO RESTRICTED	NATO CONFIDENTIAL	NATO	COSMIC		TECT		CONFIDENTIAL	SECRET	TOP SECRET
				CONFIDENTIEL		TRÉS SECRET	NATO DIFFUSION RESTREINTE	NATO CONFIDENTIEL		SECRET COSMIC TRÉS SECRET	A	В	С	CONFIDENTIEL		TRES SECRET
Information / Assets Renseignements / Biens																
Production											Т					
IT Media / Support TI		П														
IT Link / Lien électronique																
12. a) Is the descrip La description If Yes, classif Dans l'affirma « Classificatic	du t y th stive	rava Is fo	ill vis irm l assif	é par la prése ny annotating ier le présent	the top a	S est-elle and botto re en ind	de nature P m in the are iquant le niv	ROTÉGÉE et a entitled "So	ou CLAS	lassificati		áe			√ No Non	Yes
12. b) Will the docu La documenta	men	tatio	n att	ached to this	SRCL be	PROTEC	TED and/or (√ No Non	Yes
If Yes, classifi attachments (Dans l'affirma	e,g.	SE	CRE	T with Attach	ments).				•				Indic	ate with		

« Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des plèces jointes (p. ex. SECRET avec

des pièces jointes).



Gouvernement du Canada

Contract	Number	1	Numéro	die	contrat
Commaci	MANITORI	,	HUITICIO	uu	CUITILI GI

W6369-17-P5LA S2 Americanent 1
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 CONTRA	CTUELLE	EO A EA GEOGRITE (EVERG)
1. Originating Government Department or Organization	on /		2. Branch or Directorate / Direction générale ou Direction
Ministère ou organisme gouvernemental d'origine	DND		DGIMTSP / DIMEI
3. a) Subcontract Number / Numéro du contrat de so	us-traitance 3. b) N	ame and Addres	ss of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work / Brève description du tra	avail		
Professional services using the Task-Based Informatics	Professional Services (TBIPS)	supply arrangemen	ant on an as-required basis.
5. a) Will the supplier require access to Controlled Go Le fournisseur aura-t-il accès à des marchandis			No V Y
5 b) Will the supplier require access to unclassified r	nilitary technical data subje	ct to the provision	
Regulations?			Non V O
Le fournisseur aura-t-il accès à des données ter	chniques militaires non clas	sifiées qui sont a	assujettles aux dispositions du Réglement
sur le contrôle des données techniques? 6. Indicate the type of access required / Indiquer le type	ma d'acrès sagule		
 a) Will the supplier and its employees require acce Le fournisseur ainsi que les employés auront-ils 	ss to PROTECTED and/or	CLASSIFIED Info	nformation or assets?
(Specify the level of access using the chart in Q	uestion 7 c)	its ou a des bien	ns PROTEGES et/ou CLASSIFIES?
Préciser le niveau d'accès en utilisant le tablea	u qui se trouve à la question	n 7. c)	
b) Will the supplier and its employees (e.g. cleaner	s, maintenance personnel)	require access to	to restricted access areas? No access to / No Ye
PROTECTED and/or CLASSIFIED information of	or assets is permitted.		Non L O
Le fournisseur et ses employés (p. ex. nettoyeur à des renseignements ou à des biens PROTÉG	rs, personnel d'entretien) at És atlau CLASSIEIÉS n'er	tront-ils acces a	des zones d'accès restreintes? L'accès
6. c) Is this a commercial courier or delivery requirem	ent with no overnight stora	ne?	I No Ye
S'agit-il d'un contrat de messagerie ou de livrais	on commerciale sans entre	posage de nuit?	? VonO
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 / OTA	NV	Foreign / Étranger
7. b) Release restrictions / Restrictions relatives à la	diffusion		
No release restrictions	All NATO countries		No release restrictions
Aucune restriction relative	Tous les pays de l'OTAN		Aucune restriction relative
a la diliusion			a la diliusion
Not releasable			
A ne pas diffuser			
Restricted to: / Limité à :	Restricted to: / Limité à :		Restricted to: / Limité à :
Specify country(ies): / Préciser le(s) pays :	Specify country(les): / Pré	ciser le(s) pays	Specify country(ies): / Préciser le(s) pays :
	CANADIAN	CITIZEN	21.
	CHUMBIMP	CHITCH	93
7. c) Level of information / Niveau d'information			
PROTECTED A	NATO UNCLASSIFIED		PROTECTED A
PROTÉGÉ A PROTECTED B	NATO NON CLASSIFIÉ NATO RESTRICTED		PROTÉGÉ A L. PROTECTED B
PROTÉGÉ B	NATO DIFFUSION REST	REINTE	PROTÉGÉ B
PROTECTED C	NATO CONFIDENTIAL		PROTECTED C
PROTÉGÉ C	NATO CONFIDENTIEL		PROTÉGÉ C
CONFIDENTIAL	NATO SECRET		CONFIDENTIAL
CONFIDENTIEL	NATO SECRET	4	CONFIDENTIEL
SECRET	COSMIC TOP SECRET		SECRET
OCONC!	COSMIC TRÈS SECRET		SECRET
TOP SECRET			TOP SECRET
TRES SECRET			TRÈS SECRET
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT)			TOP SECRET (SIGINT)
THE SECRET (SIGNAT)	NEW TOTAL CONTRACTOR OF THE PARTY OF THE PAR		TRÈS SECRET (SIGINT)

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité UNCLASSIFIED

Canadä'



TBS/SCT 350-103(2004/12)

Government of Canada Gouvernement du Canada

Contract Number / Numéro du contrat W6369-17-P5LA S2

Security Classification / Classification de sécurité UNCLASSIFIED

Canadä'

PART A (continued) / PARTIE A (suite) 8. Will the supplier require access to PROTECTED and/or CLAS Le fournisseur aura-t-il accès à des renseignements ou à des If Yes, indicate the level of sensitivity: Dans l'affirmative, indiquer le niveau de sensibilité: 9. Will the supplier require access to extremely sensitive INFOSI Le fournisseur aura-t-il accès à des renseignements ou à des	biens COMSEC désignation or ass	ets?	BIFIÉS?	No Non Ves Non Ves Non Oui
Short Title(s) of material / Titre(s) abrégé(s) du matériel : Document Number / Numéro du document :				
PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNE 10. a) Personnel security screening level required / Niveau de co	EL (FOURNISSEUR) ontrôle de la sécurité d	du personnel requis	A L	
RELIABILITY STATUS CONF	FIDENTIAL	SECRET SECRET	TOP SECR TRÈS SECR	RET
	CONFIDENTIAL CONFIDENTIEL	NATO SECRET NATO SECRET		OP SECRET RÈS SECRET
SITE ACCESS ACCÈS AUX EMPLACEMENTS				
Special comments: Commentaires spéciaux :				
NOTE: If multiple levels of screening are identified REMARQUE: Si plusleurs niveaux de contrôle	d, a Security Classifica de sécurité sont requi	tion Guide must be provided. s, un guide de classification de	la sécurité doit être f	ourni.
10. b) May unscreened personnel be used for portions of the wo Du personnel sans autorisation sécuritaire peut-il se voir of	rk?			✓ Non Yes Oui
If Yes, will unscreened personnel be escorted? Dans l'affirmative, le personnel en question sera-t-il escor				No Yes Non Oui
PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURE	S DE PROTECTION	(FOURNISSEUR)		经验证证据
INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS				
11. a) Will the supplier be required to receive and store PROTE premises? Le fournisseur sera-t-il tenu de recevoir et d'entreposer su CLASSIFIÉS?				Von Ves Non Oui
Will the supplier be required to safeguard COMSEC information. Le fournisseur sera-t-il tenu de protéger des rensalgnements.	nation or assets?	MSEC?		Ves Non Ves Oui
PRODUCTION				
				¥ 257
11. c) Will the production (manufacture, and/or repair and/or modifioccur at the supplier's site or premises? Les installations du fournisseur serviront-elles à la productio et/ou CLASSIFIÉ?				Vo Non Ves Oui
INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RE	LATIF À LA TECHNO	LOGIE DE L'INFORMATION (T	1)	
11. d) Will the supplier be required to use its IT systems to electron information or data? Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes renselgnements ou des données PROTÉGÉS et/ou CLASS	Informatiques pour trai			No Yes Non Oui
11. e) Will there be an electronic link between the supplier's IT syst Disposera-t-on d'un lien électronique entre le système information gouvernementale?	ems and the governmentique du fournisseur	ent department or agency? et celui du ministère ou de l'age	nce	No Yes Non Oul

Security Classification / Classification de sécurité

UNCLASSIFIED



Gouvernement du Canada Contract Number / Numéro du contrat

W6369-17-P5LA S2

Security Classification / Classification de sécurité
UNCLASSIFIED

									STORY OF STREET	SHANNER OF THE	1515000		130000		41576	STATE OF THE PARTY
ART C - (continue	d) []	PAR	TIE	C - (suite)	ALCOHOL: N	No. of the last of	t halau ta !	diente the coto	annilles)	and level	(s) of	safe	nuar	dina required	at the sur	polier's
For users comple		the	orm	manually use	the sum	mary chai	t below to the	licate the cate	gury(ies)	and icve	(3) (1	3010	3001	and rodoned	501	-1
site(s) or premise Les utilisateurs q	2S.			t la formulaira	manualle	ement do	went utiliser	le tableau réc	anitulatif (ci-dessous	s pour	Indi	quer	, pour chaque	catégorie	e, les
niveaux de sauvi	in te	mpii	ssen	ellationniol el ji	ne du fou	rnisseur	IACLIC OURSE.	10 100,000 100					,		-	
For users comple	etina	the	form	online (via th	e Internet), the sun	nmary chart is	s automaticall	y populat	ed by you	r resp	onse	s lo	previous que	stions	1.1.
Por users comple Dans le cas des	utilis	ateu	rs qu	ui remplissent	le formula	ire en lig	ne (par Inter	net), les répor	ises aux	questions	précé	deni	es s	ont automatic	luement s	aisies
dans le tableau r	écap	itula	tif.													
					SL	IMMARY	CHART /	TABLEAU R	ECAPIT	JEATIF						
				- 11 11 11 11 11 11 11 11 11 11 11 11 11							_					
				CI	SSIFIED			NATO						COMSEC		
Category Catégorie		OTECT			ASSIFIÉ											
	-	Т	1		I	TOP	NATO	NATO	NATO	COSMIC		TECT				TOP
	A	В	C	CONFIDENTIAL	SECRET	SECRET	RESTRICTED	CONFIDENTIAL	SECRET	TOP	PR	OTEG		CONFIDENTIAL	SECRET	SECRET
				CONFIDENTIEL		TRES	NATO	NATO		COSMIC	A	В	С	CONFIDENTIEL.		TRES
						SECRET	DIFFUSION RESTREINTE	CONFIDENTIEL		TRÉS SECRET						SECRET
Information / Assets	+-		-			-	RESTREMIE		1	GEGGE	1				1	
Renseignements / Bien	s								-	-	+-	-	-		-	
Production																
IT Media /	+	+														
Support TI	+-	+	-		-	-	-	-		-	1					
Lien électronique		1												L		
12. a) Is the descri	iption	n of t	he w	ork contained	within this	s SRCL P	ROTECTED	and/or CLAS	SIFIED?	cciEiÉE?				A. A	√ No Non	Yes
La description	n du	trava	all vis	sé par la prése	enie LVEF	S est-ell	e de nature P	KUIEGEE BI	IUG CLAS	JOHN ILLE				L	.4011	
if Yes, classi	S. 45	in de	vers 1	hy annotation	the ton	and hotte	om in the are	a entitled "S	ecurity C	lassificat	ilon".					
Dane Paffirm	ny u	a cl	acci:	fier le présen	formula	ire en inc	liquant le ni	veau de sécu	rité dans	la case i	ntitul	ée				
a Classificat	lon	ie s	cur	lté » au haut	et au bas	du form	ulaire.									
														ſ	. No	Yes
12. b) Will the doc	ume	ntati	on at	tached to this	SRCL be	PROTEC	CTED and/or	CLASSIFIED	? SIEIĖE?						Non	Oui
La document	ation	855	ocié	e à la présent	LVERS	sera-i-elle	PRUIEGE	E enon crass	SIFIEL					,	14041	
attachments Dans l'affirm « Classificat	(e.g nativ	. SE e, cl de s	CRE	by annotating T with Attacl fler le présen ité » au haut	iments).	iro on in	diament le ni	veau de sécu	rité dans	la case i	ntitu	ée				
des plèces j	OINTO	15).														

Security Requirement Checklist (SRCL) Supplemental Security Guide

Part A - Multiple Release Restrictions: Security Guide

				Canadia	n Information					
Citizenship Restriction	PF	ROTE	CTED			ASSIFIED				
Restriction	А	В	С	CONFIDENTIAL	L SECRET	TOP SECRE	TOP SECRET			
No Release Restrictions	X	X								
Not Releasable										
Restricted to: CAN/US				X	X					
Permanent Residents Included*										
				NATO	Information					
Citizenship Restriction	UN	NATO CLASSI		NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET			
All NATO Countries										
Restricted to: CAN / US						Х				
Permanent Residents Included*										
			r vije	Foreign	Information					
Citizenship	PROTECTED			CLASSIFIED						
Restriction	A	В	С	CONFIDENTIAL	SECRET	TOP SECRE	T TOP SECRET (SIGINT)			
No Release Restrictions										
Restricted to :										
Permanent Residents Included*										
		60 45 1		COMSEC	Information					
Citizenship Restriction	PR	OTEC	TED		CL	ASSIFIED				
Restriction	Α	В	С	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)			
Not Releasable		1								

^{*}When release restrictions are indicated, specify if permanent residents are allowed to be included.

Security Requirement Checklist (SRCL) Supplemental Security Guide

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, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
NATO SECRET	CHANGE MANAGEMENT CONSULTANT (LEVEL 3)	UP TO AND INCLUDING NATO SECRET	CANADIAN OR US CITIZEN
NATO SECRET	PROJECT MANAGER (LEVEL 3)	UP TO AND INCLUDING NATO SECRET	CANADIAN OR US CITIZEN
NATO SECRET	PKI SPECIALIST (LEVEL 2 AND 3)	UP TO AND INCLUDING NATO SECRET	CANADIAN OR US CITIZEN
NATO SECRET	IT SECURITY ENGINEER (LEVEL 1, 2, 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

While the protected A/B information itself has no release restrictions, all personnel working on this contract must be Canadian or US citizens.

Security Requirement Checklist (SRCL) Supplemental Security Guide

WG3G9 17 PSLA - S2
Part A - Multiple Release Restrictions: Security Guide

Citizenship Restriction No Release Restrictions Not Releasable Restricted to: Permanent Residents Included*	A X	B X	CTED	CONFIDENTIA			ASSIFIED TOP SECR	ET TOP SECR (SIGINT
No Release Restrictions Not Releasable Restricted to: Permanent Residents	X		С			RET	TOP SECR	TOF SECR
Not Releasable Restricted to: Permanent Residents	11717	X		Х				
Restricted to: Permanent Residents	1161			Х				
Permanent Residents	1161				X		X	Х
	1181							
	1161							
	1161			NATO	Information			
Citizenship Restriction	UNI	NATO CLASSIF		NATO RESTRICTED	NATO CONFIDE	ENTIAL	NATO SECRET	COSMIC TOP SECR
All NATO Countries								
Restricted to: CANADIAN CITIZENS							Х	
Permanent Residents Included*								
	1.43%	1		Foreig	n Information	n		
Citizenship	PR	OTEC	TED			CLA	SSIFIED	
Restriction	Α	В	С	CONFIDENTIA	L SECR	RET	TOP SECRE	TOP SECRI (SIGINT)
No Release Restrictions								
Restricted to :				8				
Permanent Residents Included*								
			Tell X	COMSE	C Informatio	n		
Citizenship	PR	OTEC	TED			CLA	SSIFIED	
Restriction	А	В	С	CONFIDENTIA	L SECR	ET	TOP SECRE	TOP SECRE
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

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.

personnei screen	ing levels are required for which	portions of the work/access involved in	the contract
Level of Personnel Clearance (e.g. Reliability, 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 TRA AND C&A ANALYST (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	PKI SPECIALIST (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	IT SECURITY ENGINEER (LEVEL 1, 2, 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	IT SECURITY DESIGN SPECIALIST (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	NETWORK SECURITY ANALYST (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	IT SECURITY SYSTEMS OPERATOR (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	IT SECURITY VA SPECIALIST (LEVEL 3)	UP TO AND INCLUDING TS- SIGINT	CANADIAN CITIZEN
NATO SECRET AND TOP SECRET -SIGINT	INCIDENT MANAGEMENT SPECIALIST (LEVEL) 3	UP TO AND INCLUDING TS- 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

OTHER SECURITY INTRUCTIONS

Insert instructions

While the protected A/B information itself has no release restrictions, all personnel working on this contract must be Canadian citizens.

PIÈCE JOINTE 4.1 CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 1 – SECRET

- Les critères d'évaluation de la présente pièce jointe serviront à évaluer les soumissions dans le cadre de la demande de soumissions et à faciliter l'évaluation des ressources après l'attribution du contrat.
- 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 à la présente demande de soumissions). ď
- Le soumissionnaire doit remplir une grille d'évaluation pour chacun des curriculum vitæ fournis, tel que 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. က

Tableau 1 : Le soumissionnaire doit soumettre le nombre suivant de ressources par catégorie en réponse à la présente évaluation. Les nombres réels de ressources requises figurent au point 1.2, Résumé, de la demande de soumissions.

Catégorie de ressources	Niveau	Nombre de curriculum vitæ
P.1 Expert-conseil en gestion du changement	3	1
P.9 Gestionnaire de projet	æ	Τ
C.5 Spécialiste de l'Infrastructure à clés publiques (ICP)	2	1
C.5 Spécialiste de l'ICP	33	
C.6 Ingénieur en sécurité des TI	П	П
C.6 Ingénieur en sécurité des TI	2	1
C.7 Spécialiste en conception de la sécurité des TI	2	1
C.7 Spécialiste en conception de la sécurité des TI	3	1

1. EXIGENCES RELATIVES À L'ENTREPRISE

1.1. Exigences obligatoires relatives à l'entreprise

	EXIGENCES OBLIGATOIRES – CRITÈRES RELATIFS À L'ENTREPRISE	ISE	
Point		RESPECTÉ (oui/non)	Nos de page dans le document de soumission
10	Le soumissionnaire doit s'être fait octroyer au moins deux (2) contrats de services professionnels en informatique¹ 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 de la présente demande de soumissions 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. Chaque contrat mentionné doit également démontrer 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 référence 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 l'engagement du soumissionnaire consistait à réaliser des travaux qui faisaient partie d'un contrat conclu par une autre entité, le soumissionnaire ne serait pas considéré comme l'entrepreneur principal. Par exemple, Z (le client) attribue à Y un contrat de services. Y, à son tour, a engagé X pour lui fournir une partie ou la totalité des services demandés par Z. Dans cet exemple, Y est l'entrepreneur principal et X est un 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, 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.	*On entend par client gouvernemental un ministère ou un organisme fédéral, provincial ou municipal ou 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 contrat en technologie ou en gestion de l'information.

CRITÈRES D'ÉVALUATION DES RESSOURCES

CRITÈRES OBLIGATOIRES

•	•	•	
	_	4	
	-	•	
	000	3	
	۵	١	
	5		
	F		
	5	7	
í	_	4	
		Ċ	
	Changanan	4	
	Ξ	ŧ	
	Q	J	
	c	3	
	ς	3	
	a	Ċ	
	Ē	'n	
	≥	٣	
	Σ	₹.	
		3	
	č	ĭ	
	•	┥	
	C	J	
	_	•	
	-	٠	
	=	3	
	⊆	3	
	7	Ξ.	
	≥	_	
,	Ξ	3	
	Ż	n	
	ă	3	
	Ē	'n	
	on opertion	w	
	_	1	
	2	•	
	a	,	
	2	1	
	ā	•	
		3	
,	_	₹	
	q	3	
	Ū	2	
	222	₹.	
	2	7	
	Ç	ڔ	
)	
•	·	•	
		4	
۲	_	7	
	١	Ĭ	

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, FTC.)
	P.1 Conseiller en gestion du changement – Niveau 3	t – Niveau 3		
\circ	O1 Le soumissionnaire doit prouver que la			
	ressource proposée possède : soit au moins dix (10) années d'expérience combinée à			
	titre de conseiller en gestion du			
	changement au cours des			
	quinze (15) dernières années, soit au			
	moins (5) années d'experience a titre de conseiller en oestion du changement au			
	cours des dix (10) dernières années			
	accompagnées d'au moins trois (3) des			
	accréditations professionnelles reconnues			
	des suivantes :			
	Association of Change Management			
	Professionals (ACMP);			
	 Project Management Professional 			
	(PMP);			
	 Certified Associate in Project 			
	Management (ACMP);			
	Program Management Professional			
	(PgMP);			
	 Portfolio Management Professional 			
	(PfMP);			
	 Agile Certified Practitioner (PMI- 			
	ACP);			
	 PMI Professional in Business 			
	Analysis (PMI-PBA);			
	PMI Risk Management Professional			

		(PMI-RMP); et • PMI Scheduling Professional (PMI-SP);	
	Unc	Une copie des certifications valides de la ressource doit être jointe à la soumission.	
07	2 Le ress cin cin plan plan sup cha cha con con con sup sup cha con	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans la planification, l'évaluation, le suivi et la supervision d'activités de gestion du changement, ainsi que la formulation de conseils à cet égard.	
	Cor	Conforme (oui/non)?	

Niveau 3
projet –
stionnaire de
Gestion
P.9

			INOIN	MOTETE DOGOTAL A PINA A PLOAGINE, SEAT A PINETARION
	ENIGENCE	KESFECIEE	RESPECTÉE	COMMENTALKES (ENDROLL DANS LA FROFOSILLON, CRITÈRES NON SATISFAITS, ETC.)
	P.9 Gestionnaire de projet – Niveau 3			
	O1 Le soumissionnaire doit prouver que la			
	ressource proposée possède soit au moins			
	titre de gestionnaire de proiet au cours des			
	quinze (15) dernières années, soit au			
	moins (5) années d'expérience à titre de			
	gestionnaire de projet au cours des			
	dix (10) dernières années et au moins			
	trois (3) accréditations professionnelles			
	reconnues des suivantes :			
	Project Management Professional			
	(PMP);			
	 Certified Associate in Project 			
	Management (CAPM);			
	Program Management Professional			
	(PgMP);			
	 Portfolio Management Professional 			
	(PfMP);			
	• Agile Certified Practitioner (PMI-			
	ACF),			
	 PMI Professional in Business Analysis (PMI-PBA): 			
	PMI Risk Management Professional			
	(PMI-RMP); et			
	• PMI Scheduling Professional (PMI-			
	SP);			
	Une conje des certifications valides de la			
	ressource doit être jointe à la soumission.			
['	+			
	O2 Le soumissionnaire doit démontrer que la			
ل	Toggation proposed possess as mount			

Conforme (oui/non)?	
Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience acquise au cours des dix (10) dernières années dans l'élaboration et la tenue à jour de plans de projet, d'échéanciers, de coûts et de ressources à l'aide de Microsoft Project 2013 (ou d'une version plus récente).	03
cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans la planification, l'évaluation, le suivi et la supervision d'activités d'une équipe de projet, ainsi que la formulation de conseils à cet égard.	

C.5 Spécialiste de l'ICP – Niveau 2

	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,	RESPECTÉE CRITÈRES NON SATISFAITS, ETC.)
	NON	RESPECTÉE
	RESPECTÉE	
Cis Specialiste de l'Alleau 2	EXIGENCE	
•		

O2 L d d d d d d d d d d d d d d d d d d	C.5 Spécialiste de l'ICP – Niveau 2 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 dans la mise en œuvre et le soutien de solutions d'ICP. O2 Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des	RESPECTÉE	RESPECTÉE CRITÈRES NON SATISFAITS, ETC.)
C.5 Sylvania	s s s		
C.5.5 01	n s s s s		
O	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dermières années dans la mise en œuvre et le soutien de solutions d'ICP. Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans la mise en œuvre et le soutien de solutions d'ICP. Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	cinq (5) années d'expérience acquise au cours des dix (10) dernières années dans la mise en œuvre et le soutien de solutions d'ICP. Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	cours des dix (10) dernières années dans la mise en œuvre et le soutien de solutions d'ICP. Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	d'ICP. Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
	ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
2 7	ressource proposée possède au moins deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
ਰੋ ਹੋ	deux (2) années d'expérience combinée dans la rédaction d'au moins deux (2) des		
7	dans la rédaction d'au moins deux (2) des		
3			
t	types de documents d'ingénierie des		
S	systèmes suivants :		
	 spécifications de la conception du 		
	système;		
	 documents sur la conception et la 		
	configuration;		
	 concept d'opération (CONOP); 		
	 plans de mise en œuvre de 		
	systèmes;		
	• plans et rapports de mises à		
	l'essai;		
	 plans de soutien du cycle de vie. 		
(
<u> </u>	Conforme (oui/non)?		

3
ä
veau
7
Ī
$\mathbb{C}\mathbf{P}$
Ξ
~
ğ
iste
Ħ
:5
pé
S
Ň

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,
			RESPECTÉE	RESPECTÉE CRITÈRES NON SATISFAITS, ETC.)
C	C.5 Spécialiste de l'ICP – Niveau 3			
01	Le soumissionnaire doit démontrer que la			
	ressource proposée possède au moins			
	dix (10) années d'expérience acquise au			
	cours des quinze (15) dernières années			
	dans la mise en œuvre et le soutien de solutions d'ICP.			
07	-			
	ressource proposée possède au moins			
	trois (3) années d'expérience combinée			
	dans la rédaction d'au moins trois (3) des			
	types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception du 			
	système;			
	 documents sur la conception et la 			
	configuration;			
	• CONOP;			
	 plans de mise en œuvre de 			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	Conforme (oui/non)?			

v.
α
\geq
\subset
=
,

COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)	
NON RESPECTÉE	
au 1 RESPECTÉE	
C.6 Ingénieur en sécurité des TI – Niveau 1 EXIGENCE RE	 C.6 Ingénieur en sécurité des TI – Niveau 1 Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience acquise au cours des cinq (5) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins un (1) des domaines suivants : Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.
C.6	O1

suivants:

02

		0	The state of the state of	()	
		EXIGENCE	KESPECIEE		COMMENTALKES (ENDROIT DANS LA PROPOSITION,
				RESPECTEE	CRITERES NON SATISFAITS, ETC.)
	C.6	C.6 Ingénieur en sécurité des TI – Niveau 2	ıu 2		
_	01				
		ressource proposee possede au moins			
		cinq (5) années d'expérience acquise au			
	-	cours des dix (10) dernières années dans			
		l'élaboration et la mise en œuvre			
		d'applications et d'infrastructures de			
		sécurité des TI dans au moins deux (2) des			
		domaines suivants:			
		Systemes de prevention des			
		intrusions au niveau de l'hôte			
		(HIPS);			
		 Technologies de sécurité de 			
		réseautage sans fil;			
		• Systèmes de détection d'intrusion			
		(IDS);			
		 Systèmes de prévention des 			
		intrusions dans un réseau (IPS);			
		 Gestion de l'information et des 			
		incidents de sécurité (SIEM);			
		 Saisie intégrale de paquet (FPC); 			
		 Contrôle de l'accès au réseau 			
		(NAC);			
		 Gestion de l'identité, des 			
		justificatifs d'identité et de			
		l'accès (ICAM); et/ou			
		 Protection des terminaux. 			

	EXIGENCE	RESPECTEE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,
			RESPECTÉE	CRITÈRES NON SATISFAITS, ETC.)
)	O2 Le soumissionnaire doit démontrer que la			
	ressource proposée possède au moins			
	deux (2) années d'expérience combinée			
	dans la rédaction d'au moins deux (2) des			
	types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception du 			
	système;			
	documents sur la conception et la			
	configuration;			
	• CONOP;			
	• plans de mise en œuvre de			
	systèmes;			
	 plans et rapports de mises à 			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	Conforme (oui/non)?			
	_		_	

C.7 Spécialiste en conception de sécurité des TI – Niveau 2

_از	C./ Specialiste en conception de securit	IIIC UCS II — Miveau 2 PFSDFCTFFF	au 2	COMMENTATRES (FUNDOIT DANS I A PROPOSITION
	PAIGENCE	MESI ECTEE	TÉE	CRITÈRES NON SATISFAITS, ETC.)
ပ်	C.7 Spécialiste en conception de sécurité des TI – Niveau 2	té des TI – Nive	au 2	
01	Le soumissionnaire doit démontrer que la			
	cinq (5) années d'expérience acquise au			
	cours des dix (10) dernieres années dans la planification et la mise en œuvre			
	d'architectures d'intégration de la sécurité des TI.			
07	2 Le soumissionnaire doit démontrer que la			
	ressource proposée possède au moins			
	deux (2) années d'expérience combinée			
	dans la rédaction d'au moins deux (2) des			
	types de documents d'ingénierie des			
	systèmes suivants :			
	 spécifications de la conception du 			
	système;			
	 documents sur la conception et la 			
	configuration;			
	• CONOP;			
	 plans de mise en œuvre de 			
	systèmes;			
	• plans et rapports de mises à			
	l'essai;			
	 plans de soutien du cycle de vie. 			
	6();)			
	Conforme (out/non)?			
			-	

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
C	C.7 Spécialiste en conception de sécurit	rité des TI – Niveau 3		
01	Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans la planification et la mise en œuvre d'architectures d'intégration de la sécurité des TI.			
00	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée dans la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans et rapports de mises à l'essai; • plans de soutien du cycle de vie.			
	Conforme (oui/non)?			

CRITÈRES COTÉS

P.1 Conseiller en gestion du changement – Niveau 3

	1.1 Conscinct on gestion an changement – Mycau 3	icii – Mycau J			
$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
P.1 C	P.1 Conseiller en gestion du changen	nent – Niveau 3			
C1	Le soumissionnaire doit montrer que	1 point = de 1 à 3 années d'expérience	4		
		2 points = plus de 3 à 5 années			
	l'expérience dans la rédaction de	d'expérience			
	documents de gestion de projet à	3 points = plus de 5 à 8 années			
	l'aide des lignes directrices du	d'expérience			
	Project Management Body of	4 points = plus de 8 années			
	Knowledge (référentiel des	d'expérience			
	connaissances en gestion de proiet).				
C2	Le soumissionnaire doit montrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
		d'expérience			
	util,	3 points = plus de 5 à 8 années			
		d'expérience			
		4 points = plus de 8 années			
		d'expérience			
C3	Le soumissionnaire doit montrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
	l'expérience dans la direction et	d'expérience			
	l'animation de réunions, de groupes	3 points = plus de 5 à 8 années			
	de travail et de discussions, ainsi	d'expérience			
	que dans la préparation d'exposés et	4 points = plus de 8 années			
	leur présentation à divers	d'expérience			
	intervenants.				

RÉFÉRENCE À LA	PROPOSITION (PAGE ET				
NOTE					
MAX.	DE	4	4	4	Note maximale: 24 points
BARÈME DE NOTATION		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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	Note de passage minimale : 14 points
CRITÈRES		Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans la conduite d'analyses des répercussions du changement et d'activités de gestion du changement.	Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans la gestion d'autres employés afin de définir les stratégies et les processus opérationnels permettant de favoriser les transformations et les activités de gestion du changement.	Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans la réalisation de vérifications des processus de gestion de la configuration et du changement.	Total:
$\overset{\circ}{\mathbf{Z}}$		C4	S	92	

P.9 (P.9 Gestionnaire de projet – Niveau	3			
$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
P.9	P.9 Gestionnaire de projet – Niveau	3			
C1	Le soumissionnaire doit démontrer	1 point = de 1 à 3 années d'expérience	4		
	que la ressource proposée possède	2 points = plus de 3 à 5 années			
	de l'expérience dans la gestion d'au	d'expérience			
	moins deux (2) gestionnaires de	3 points = plus de 5 à 8 années			
	projet, chacun étant responsable	d'expérience			
	d'un élément lié à un projet et de	4 points = plus de 8 années			
	l'équipe de projet connexe.	d'expérience			
C2	Le soumissionnaire doit montrer que	1 point = de 1 à 3 années d'expérience	4		
	la ressource proposée possède de	2 points = plus de 3 à 5 années			
	l'expérience dans la rédaction de	d'expérience			
	documents de gestion de projet à	3 points = plus de 5 à 8 années			
	1'aide des lignes directrices du	d'expérience			
	Project Management Body of	4 points = plus de 8 années			
	Knowledge (référentiel des	d'expérience			
	connaissances en gestion de projet).				

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)		
NOTE		
MAX. DE POINTS	4	4
BARÈME DE NOTATION	3 projets = 1 point 4 projets = 2 points 5 projets = 3 points 6 projets = 4 points	3 projets = 1 point 4 projets = 2 points 5 projets = 3 points 6 projets = 4 points
N° CRITÈRES	Le soumissionnaire doit montrer que la ressource proposée a acquis, au cours des cinq (5) demières années, de l'expérience dans la gestion de projets de GI-TI aux phases d'élaboration ou de mise en œuvre à l'aide de Microsoft Project afin de garantir que les ressources sont disponibles et que le projet est conçu et entièrement fonctionnel. Pour être prise en compte, l'expérience doit avoir été d'au moins six (6) mois.	Le soumissionnaire doit montrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, de l'expérience dans la détermination et la documentation des jalons des projets de GI-TI, la détermination des exigences budgétaires, la constitution d'équipes de projet, ainsi que la définition des rôles, des responsabilités et du mandat des membres des équipes. Pour être prise en compte, l'expérience doit avoir été d'au moins six (6) mois.
$\overset{\circ}{\mathbf{Z}}$	C3	C4

RÉFÉRENCE À LA	PROPOSITION (PAGE ET PARAGRAPHE)					
NOTE						
MAX.	DE POINTS	4	4	4	4	Note maximale: 32 points
BARÈME DE NOTATION		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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	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 8 années d'expérience 4 points = plus de 8 années d'expérience	Note minimale de passage : 19 points
N° CRITÈRES		Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans la gestion de l'information au moyen d'un outil, comme SharePoint.	Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans la direction et l'animation de réunions, de groupes de travail et de discussions, ainsi que dans la préparation d'exposés et leur présentation à divers intervenants.	Le soumissionnaire doit montrer que la ressource proposée a de l'expérience en matière d'élaboration et de gestion d'un plan d'activités.	Le soumissionnaire doit montrer que la ressource proposée possède de l'expérience dans le lancement et la gestion de l'approvisionnement, ainsi que la gestion de contrat de sécurité des TI.	Total:
$\overset{\circ}{\mathbf{Z}}$		හි	90	C7	C8	

21/38

C.5 Spécialiste de l'ICP – Niveau 2

4	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA	
			DE		PROPOSITION (PAGE ET	
			POINTS		PARAGRAPHE)	
	C.5 Spécialiste de l'ICP – Niveau 2					
	Le soumissionnaire doit montrer que	1 point = minimum d'expérience	5			
	la ressource possède au moins	combinée démontrée avec une (1) des				
	trois (3) années d'expérience	technologies énoncées dans un				
	combinée dans l'examen, l'analyse,	contexte d'ICP				
	la mise en œuvre et le soutien des	2 points = minimum d'expérience				
	technologies suivantes dans un	combinée démontrée avec deux (2)				
	contexte d'ICP:	des technologies énoncées dans un				
		contexte d'ICP				
	1) architectures d'ICP;	3 points = minimum d'expérience				
	2) signatures numériques et	combinée démontrée avec trois (3)				
	chiffrement;	des technologies énoncées dans un				
	3) produits d'ICP, notamment	contexte d'ICP				
	l'autorité de certification et	4 points = minimum d'expérience				
	l'autorité d'enregistrement;	combinée démontrée avec quatre (4)				
	4) produits reposant sur des clés	des technologies énoncées dans un				
	publiques, comme les réseaux	contexte d'ICP				
	privés virtuels, la voix par le	5 points = minimum d'expérience				
	protocole Internet et l'extension	combinée démontrée avec cinq (5) ou				
	S/MIME;	plus des technologies énoncées dans				
	5) produits d'annuaire X.500;	un contexte d'ICP				
	6) normes de certificat X.509;					
	7) protocoles de sécurité Internet;					
	8) produits du protocole de					
	vérification en ligne de l'état des					
	certificats.					

\mathbf{Z}°	CRITÈRES	BARÈME DE NOTATION MAX. NOTE RÉFÉRENCE À LA	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

0	0
5	Ò
V	ñ
C	1

|--|

$\overset{\circ}{\mathbf{Z}}$	CRITERES	BAREME DE NOTATION	MAX. DE	NOTE	REFERENCE A LA PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C4	Le soumissionnaire doit démontrer que la ressource proposée a travaillé pendant au moins cinq (5) années avec les produits/solutions d'ICP cidessous: 1) autorité de certification Entrust; 2) autorité de certification Microsoft; 3) modules de sécurité matérielle; 4) solutions de gestion des cartes; 5) cartes à puce et logiciels des cartes à puce; 6) logiciel client Entrust.	1 point = minimum d'expérience combinée démontrée avec un (1) des produits/solutions d'ICP énumérés 2 points = minimum d'expérience combinée démontrée avec deux (2) des produits/solutions d'ICP énumérés 3 points = minimum d'expérience combinée démontrée avec trois (3) des produits/solutions d'ICP énumérés 4 points = minimum d'expérience combinée démontrée avec quatre (4) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec quatre (4) des produits/solutions d'ICP énumérés 5 points = minimum d'expérience combinée démontrée avec cinq (5) ou plus des produits/solutions d'ICP énumérés	S		
CS	Le soumissionnaire doit démontrer que la ressource proposée détient une (1) des certifications suivantes : 1) Certified Information System Security Professional (CISSP); 2) Certified Cloud Security Professional (CCSP); et/ou 3) Systems Security Certified Professional (SSCP); Une copie des certifications valides de la ressource doit être jointe à la soumission.	e nue des	7		
	Total:	Note de passage minimale : 12 points	Note maximale: 20 points		

– Niveau 1
\mathbf{I}
des
بة،
sécurité
énieur en
5 Ing
\ddot{c}

°Z	N° CRITÈRES BAF	BAREME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6 In	Ingénieur en sécurité des TI – Ni	Niveau 1			
C1	L'entrepreneur doit montrer que la	1 point = minimum d'expérience	Ŋ		
	ressource proposée possède au	combinée démontrée avec une (1) des			
	moins une (1) année d'expérience	solutions de sécurité des TI			
	combinée de l'élaboration et de la	énumérées			
	documentation de spécifications	2 points = minimum d'expérience			
	relatives aux exigences de système	combinée démontrée avec deux (2)			
	pour les solutions en matière de	des solutions de sécurité des TI			
	sécurité des TI suivantes:	énumérées			
		3 points = minimum d'expérience			
	1) Systèmes de prévention des	combinée démontrée avec trois (3)			
	intrusions au niveau de	des solutions de sécurité des TI			
	1'hôte (HIPS);	énumérées			
	2) Technologies de sécurité de	4 points = minimum d'expérience			
	réseautage sans fil;	combinée démontrée avec quatre (4)			
	3) Systèmes de détection	des solutions de sécurité des TI			
	d'intrusion (IDS);	énumérées			
	4) Systèmes de prévention des	5 points = minimum d'expérience			
	intrusions dans un réseau	combinée démontrée avec cinq (5) des			
	(IPS);	solutions de sécurité des TI			
	5) Gestion de l'information et	énumérées			
	des incidents de sécurité				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	Protection des terminaux.				

Niveau 2
Ĺ
Ė
es
ð
Ġ
:
n sécurité
en
nieur
ű
ğ
H
9
۲ ;

Š	N° CRITÈRES BAR	BAREME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6	Ingénieur en sécurité des TI – Ni	Viveau 2			
Cl	Le soumissionnaire doit démontrer	1 point = minimum d'expérience	S		
	que la ressource proposée possède	combinée démontrée avec une (1) des			
	au moins deux (2) années	solutions de sécurité des TI			
	d'expérience combinée de	énumérées			
	l'élaboration et de la documentation	2 points = minimum d'expérience			
	de spécifications relatives aux	combinée démontrée avec deux (2)			
	exigences de système pour les	des solutions de sécurité des TI			
	solutions en matière de sécurité des	énumérées			
	TI suivantes:	3 points = minimum d'expérience			
		combinée démontrée avec trois (3)			
	1) Systèmes de prévention des	des solutions de sécurité des TI			
	intrusions au niveau de	énumérées			
	l'hôte (HIPS);	4 points = minimum d'expérience			
	2) Technologies de sécurité de	combinée démontrée avec quatre (4)			
	réseautage sans fil;	des solutions de sécurité des TI			
	3) Systèmes de détection	énumérées			
	d'intrusion (IDS);	5 points = minimum d'expérience			
	4) Systèmes de prévention des	combinée démontrée avec cinq (5) des			
	intrusions dans un réseau	solutions de sécurité des TI			
	(PS);	énumérées			
	5) Gestion de l'information et				
	des incidents de sécurité				
	(SIEM);				
	6) Saisie intégrale de paquet				
	(FPC);				
	7) Contrôle de l'accès au				
	réseau (NAC);				
	8) Gestion de l'identité, des				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	9) Protection des terminaux.				

$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
C2	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (ITSG).	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		
ប	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	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 doit démontrer que la ressource proposée possède 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 à 4 années d'expérience 4 points = plus de 4 années d'expérience	4		

	$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
				DE		PROPOSITION (PAGE ET
				POINTS		PARAGRAPHE)
C5	10	Le soumissionnaire doit démontrer	2 points = preuve d'au moins une des	2		
		que la ressource proposée détient	certifications énumérées			
		une (1) des certifications suivantes:				
		1) Certified Information System				
		Security Professional (CISSP);				
		2) Certified Cloud Security				
		Professional (CCSP); and/or				
		3) Systems Security Certified				
		Professional (SSCP);				
		Une copie des certifications valides				
		de la ressource doit être jointe à la				
		soumission.				
		Total:	Note de passage minimale :	Note		
			11 points	maximale:		
				19 points		
		<u> </u>		•		

$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES BARÈME DE NOT.	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA PROPOSITION (PAGE ET
C.7 S	C.7 Spécialiste en conception de sécurité des TI	rité des TI – Niveau 2	POINTS		PAKAGKAPHE)
C1	Le soumissionnaire doit démontrer	1 point = de 1 à 2 années d'expérience	3		
	que la ressource proposée possède	2 points = plus de 2 à 3 années			
	l'expérience de l'application des	d'expérience			
	politiques du gouvernement en	3 points = plus de 3 années			
	matière de sécurité des TI à la	d'expérience.			
	rédaction d'un document de				
	planification, d'analyse ou de mise				
	en œuvre.				
C2	Le soumissionnaire doit démontrer	1 point = de 1 à 2 années d'expérience	4		
	que la ressource possède de	2 points = plus de 2 à 3 années			
	l'expérience combinée dans	d'expérience			
	l'analyse d'au moins un (1) des	3 points = plus de 3 à 4 années			
	éléments suivants :	d'expérience			
		4 points = plus de 4 années			
	1) outils et techniques de sécurité	d'expérience			
	des TI;				
	2) données de sécurité et				
	présentation d'avis et de				
	rapports;				
	3) statistiques sur la sécurité des TI.				
C3	Le soumissionnaire doit démontrer	1 point = de 1 à 2 années d'expérience	4		
	que la ressource proposée possède	2 points = plus de 2 à 3 années			
	de l'expérience dans la classification	d'expérience			
	ou la désignation du niveau de	3 points = plus de 3 à 4 années			
	sécurité des données.	d'expérience			
		4 points = plus de 4 années			
		d'expérience			

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION MAX.	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		11 points	maximale:		
			19 points		

C.7 Spécialiste en conception de sécurité des TI – Niveau 3

°N	o Celtrebec	BABEME DE NOTATION	MAV	NOTE	DÉFÉDENCE À I A
_			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.7 S	C.7 Spécialiste en conception de sécu	urité des TI – Niveau 3			
CI	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans l'application des politiques du gouvernement en matière de sécurité des TI à la rédaction des documents d'ingénierie des systèmes (conception, réalisation, essai et mise en œuvre) ou à la mise en œuvre d'une solution.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C2	Le soumissionnaire doit démontrer que la ressource possède de l'expérience combinée dans l'analyse d'au moins un (1) des éléments suivants: 1) outils et techniques de sécurité des TI; 2) données de sécurité et présentation d'avis et de rapports; 3) statistiques sur la sécurité des 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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
ව	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans les études de classification ou de désignation du niveau de sécurité des données.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

$\overset{\circ}{\mathbf{Z}}$	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			POINTS		FROFUSITION (FAGE E1 PARAGRAPHE)
C4	ts	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
ర	Le soumissionnaire doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes: 1) Microsoft Certified Architect (MCA); 2) VMware Certified Design Expert (VCDX); 3) Microsoft Certified System Engineer (MCSE); 4) Certified Information System Security Professional (CISSP); 5) Certified Cloud Security Professional (CISSP); 6) Systems Security Certified Professional (SSCP); Une copie des certifications valides de la ressource doit être jointe à la soumission.	2 points = preuve d'au moins une (1) des certifications énumérées 4 points = preuve d'au moins deux (2) des certifications énumérées des certifications énumérées	4		

$\overset{\circ}{\mathbf{Z}}$	CRITÈRES	BARÈME DE NOTATION MAX.	MAX.	NOTE	NOTE RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

PIÈCE JOINTE 4.1 CRITÈRES D'ÉVALUATION DES SOUMISSIONS

VOLET DE TRAVAIL 2 – TRÈS SECRET

- Les critères d'évaluation de la présente pièce jointe serviront à évaluer les soumissions dans le cadre de la demande de soumissions et à faciliter l'évaluation des ressources après l'attribution du contrat. .
- 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 à la présente demande de soumissions). ĸi
- 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 Le soumissionnaire doit remplir une grille d'évaluation pour chacun des curriculum vitæ fournis, tel que décrit dans le tableau 1 ci-dessous. vitæ admissible pour chaque catégorie de ressources, la soumission sera jugée non conforme. е,

Tableau 1 : Le soumissionnaire doit soumettre le nombre suivant de ressources par catégorie en réponse à la présente évaluation. Les nombres réels de ressources requises figurent au point 1.2, Résumé, de la demande de soumissions.

Catégorie de ressources	Niveau	Nombre de curriculum vitæ
C.3 Analyste de la C et A et des EMR en sécurité des TI	3	1
C.6 Ingénieur en sécurité des TI	1	1
C.6 Ingénieur en sécurité des TI	2	1
C.6 Ingénieur en sécurité des TI	3	1
C.7 Spécialiste en conception de la sécurité des TI	3	1
C.8 Analyste de la sécurité des réseaux	3	1
C.9 Opérateur de systèmes de sécurité des TI	3	1

1. EXIGENCES RELATIVES À L'ENTREPRISE

1.1. Exigences obligatoires relatives à l'entreprise

	EXIGENCES OBLIGATOIRES – CRITÈRES RELATIFS À L'ENTREPRISE	RISE	
Point	Critères obligatoires relatifs à l'entreprise	RESPECTÉ (oui/non)	Nos de page dans le document de soumission
	Le soumissionnaire doit s'être fait octroyer au moins deux (2) contrats de services professionnels 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		
	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 de la présente demande de		
01	soumissions 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.		
	doit 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. 		
	I a coumiscionnaira doit fournir una (1) référence nour chaque contrat. Chaque meuve de		
	référence 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 l'engagement du soumissionnaire consistait à réaliser des travaux qui faisaient partie d'un contrat conclu par une autre entité, 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, a engagé X pour lui fournir une partie ou la totalité des services demandés par Z. Dans cet exemple, Y est l'entrepreneur principal et X est un 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, 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.

*On entend par client gouvernemental un ministère ou un organisme fédéral, provincial ou municipal ou 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 contrat en technologie ou en gestion de l'information.

CRITÈRES D'ÉVALUATION DES RESSOURCES

CRITÈRES OBLIGATOIRES

C.3 Analyste de la certification et Accréditation (C et A) et de l'évaluation de la menace et des risques (EMR) en sécurité des TI – Niveau 3

COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)			
NON RESPECTÉE	– Niveau 3		
RESPECTÉE	R en sécurité des TI – Niveau 3 la es e de		
EXIGENCE	Analyste de la C et A et des EMI Le soumissionnaire doit démontrer que ressource proposée possède au moins dix (10) années d'expérience combinée acquise au cours des quinze (15) dernièr années à la réalisation d'EMR en matièr sécurité des TI ou en matière de C et A.	Le soumissionnaire doit démontrer que la ressource proposée possède au moins deux (2) années d'expérience acquise au cours des cinq (5) dernières années dans l'évaluation de l'application de contrôles de sécurité, de l'évaluation des menaces et des risques associés à un système de TI ou de l'interprétation et de l'application des Conseils en matière de sécurité des technologies de l'information 33 (ITSG-33).	Conforme (oui/non)?
	0.3	02	

	or information on position and the fitting to	aa T		
	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,
			RESPECTÉE	CRITÈRES NON SATISFAITS, ETC.)
	C.6 Ingénieur en sécurité des TI – Niveau 1	au 1		
Ĺ	O1 Le soumissionnaire doit démontrer que la			
	ressource proposée possède au moins			
	une (1) année d'expérience acquise au			
	cours des cinq (5) dernières années dans			
	l'élaboration et la mise en œuvre			
	d'applications et d'infrastructures de			
	sécurité des TI dans au moins un (1) des			
	domaines suivants:			
	1) Systèmes de prévention des			
	intrusions au niveau de l'hôte			
	(HIPS);			
	2) Technologies de sécurité de			
	réseautage sans fil;			
	3) Systèmes de détection d'intrusion			
	(IDS);			
	4) Systèmes de prévention des			
	intrusions dans un réseau (IPS);			
	5) Gestion de l'information et des			
	incidents de sécurité (SIEM);			
	6) Saisie intégrale de paquet (FPC);			
	7) Contrôle de l'accès au réseau			
	Ć		_	

C.6 Ingénieur en sécurité des TI – Niveau 1

(NAC);
Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou Protection des terminaux.

8

6

~
Viveau 2
ਕ
ě
=
Z
Ť
_
_
S
<u>=</u>
۰
Ë
écurité des
بۆ
S
en
3
<u>e</u>
=
Ingénieur
纽
Ξ
_
9

L				
	EXIGENCE	RESPECTEE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
	C.6 Ingénieur en sécurité des TI – Ni	iveau 2		
\cup	O1 Le soumissionnaire doit démontrer que la ressource proposée possède au moins			
	cinq (5) années d'expérience acquise au			
	cours des dix (10) dernieres annees dans l'élaboration et la mise en œuvre			
	d'applications et d'infrastructures de			
	securite des 11 dans au moins deux (z) des domaines suivants :	vo.		
	Systèmes de prévention des			
	intrusions au niveau de l'hôte			
	(HIPS);			
	2) Technologies de sécurité de			
	réseautage sans fil;			
	3) Systèmes de détection d'intrusion	Ţ,		
	(LCJ), (Yorkhman da máriantion dan			
	5) Gestion de l'information et des			
	incidents de sécurité (SIEM);			
	• 1	••		
	7) Contrôle de l'accès au réseau			
	(NAC);			
	8) Gestion de l'identité, des			
	justificatifs d'identité et de			
	l'accès (ICAM); et/ou			
	9) Protection des terminaux.			

RESPECTÉE NON COMMENTAIRES (ENDROIT DANS LA PROPOSITION, RESPECTÉE CRITÈRES NON SATISFAITS, ETC.)	veau 3	
EXIGENCE RESPE	C.6 Ingénieur en sécurité des TI – Niveau 3	ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'élaboration et la mise en œuvre d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de prévention des intrusions dans un réseau (IPS); 4) Systèmes de prévention des intrusions dans un réseau (IPS); 5) Gestion de l'information et des incidents de sécurité (SIEM); 6) Saisie intégrale de paquet (FPC); 7) Contrôle de l'accès au réseau (NAC); 8) Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou 9) Protection des terminaux.

COMMENTAIRES (ENDROIT DANS LA PROPOSITION, E CRITÈRES NON SATISFAITS, ETC.)		
NON RESPECTÉE		
RESPECTÉE		
EXIGENCE	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée dans la rédaction d' au moins trois (3) des types de documents d'ingénierie des systèmes suivants : • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de l'essai; • plans de soutien du cycle de vie.	Conforme (oui/non)?
	00	

C.7 Spécialiste en conception de sécurité des TI – Niveau 3

COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)			
RESPECTÉE NON CO RESPECTÉE CE			
EXIGENCE	C.7 Spécialiste en conception de sécurité des TI – Niveau 3 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 dans la planification et la mise en œuvre d'architectures d'intégration de la sécurité des TI.	Le soumissionnaire doit démontrer que la ressource proposée possède au moins trois (3) années d'expérience combinée dans la rédaction d'au moins trois (3) des types de documents d'ingénierie des systèmes suivants: • spécifications de la conception du système; • documents sur la conception et la configuration; • CONOP; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de mise en œuvre de systèmes; • plans de soutien du cycle de vie.	Conforme (oui/non)?
	C.7	00	

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

	EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,
			RESPECTÉE	CRITÈRES NON SATISFAITS, ETC.)
(
	C.8 Analyste de la sécurité des réseaux – Niveau 3	– Niveau 3		
0	ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) demières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes: 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.			

	EXIGENCE	RESPECTÉE	NON RESPECTÉE	COMMENTAIRES (ENDROIT DANS LA PROPOSITION, CRITÈRES NON SATISFAITS, ETC.)
00	Le soumissionnaire doit démontrer que la ressource proposée possède au moins cinq (5) années d'expérience acquise au cours des dix (10) demières années dans l'élaboration d'exigences et la conception d'applications et d'infrastructures de sécurité des TI dans au moins deux (2) des domaines suivants: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de détection d'intrusion des intrusions dans un réseau (IPS); 5) Gestion de l'information et des incidents de sécurité (SIEM); 6) Saisie intégrale de paquet (FPC); 7) Contrôle de l'accès au réseau (NAC); 8) Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou 9) Protection des terminaux.			
	Conforme (oui/non)?			

C.9 Opérateur de systèmes de sécurité des TI – Niveau 3

C.9 Opérateur de systèmes de sécurité des TI – Niveau 3 Ol Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) demières années dans l'examen, l'analyse, la mise en ceuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		EXIGENCE	RESPECTÉE	NON	COMMENTAIRES (ENDROIT DANS LA PROPOSITION,
Opérateur de systèmes de sécurii Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes: 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.				RESPECTÉE	CRITÈRES NON SATISFAITS, ETC.)
Opérateur de systèmes de sécurii Le soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes: 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.					
ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) demières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes: 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.	C.9	Opérateur de systèmes de sécurité d	les TI – Niveau	3	
Te soumissionnaire doit démontrer que la ressource proposée possède au moins dix (10) années d'expérience acquise au cours des quinze (15) demières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.					
ressource proposée au moins dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.	0	Le soumissionnaire doit démontrer que la			
dix (10) années d'expérience acquise au cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		ressource proposée possède au moins			
cours des quinze (15) dernières années dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		dix (10) années d'expérience acquise au			
dans l'examen, l'analyse, la mise en œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		cours des quinze (15) dernières années			
œuvre ou le soutien d'au moins deux (2) des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		dans l'examen, l'analyse, la mise en			
des technologies suivantes : 1) protocoles de sécurité Internet; 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation.		œuvre ou le soutien d'au moins deux (2)			
 protocoles de sécurité Internet; protocoles réseau; algorithmes cryptographiques; normes d'annuaire; renforcement de la sécurité réseau; systèmes d'exploitation. 		des technologies suivantes :			
 protocoles de sécurité Internet; protocoles réseau; algorithmes cryptographiques; normes d'annuaire; renforcement de la sécurité réseau; systèmes d'exploitation. 					
 2) protocoles réseau; 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation. 		1) protocoles de sécurité Internet;			
 3) algorithmes cryptographiques; 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation. 		2) protocoles réseau;			
 4) normes d'annuaire; 5) renforcement de la sécurité réseau; 6) systèmes d'exploitation. 		3) algorithmes cryptographiques;			
5) renforcement de la sécurité réseau;6) systèmes d'exploitation.		4) normes d'annuaire;			
6) systèmes d'exploitation.		5) renforcement de la sécurité réseau;			
		6) systèmes d'exploitation.			

CRITÈRES COTÉS

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

		PARAGRAPHE)		
	MAA. NOIE DE	POINTS	4	4
2	BAKEWE DE NOTATION	R en sécurité des TI – Niveau 3		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 8 années d'expérience 4 points = plus de 8 années
maiyste de la C et A et des EML	CKIIEKES	C.3 Analyste de la C et A et des BM		Le soumissionnaire doit démontrer que la ressource proposée possède l'expérience de l'analyse de la conception d'architectures de sécurité des TI.
	Z	C.3 A	CI	C2

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)	
NOTE			
MAX.	DE	POINTS	4
BARÈME DE NOTATION			2 points = preuve d'au moins une (1) des certifications énumérées 4 points = preuve d'au moins deux (2) des certifications énumérées des certifications énumérées
CRITÈRES			Le soumissionnaire doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : 1) Certified Information Systems Security Professional (CISSP); 2) Certified Information Systems Auditor (CISA); 3) Certified Information Security Manager (CISM); 4) ISACA Certification in Risk and Information Systems Control; and/or Systems Control; and/or Certification. Une copie des certifications valides de la ressource proposée doit être jointe à la soumission.
°			${\mathfrak S}$

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)			
NOTE			
MAX. DE POINTS	2	4	Note maximale: 18 points
BARÈME DE NOTATION	2 points = preuve d'au moins une des certifications énumérées	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 8 années d'expérience 4 points = plus de 8 années d'expérience	Note de passage minimale : 11 points
CRITÈRES	Le soumissionnaire doit démontrer que la ressource proposée a suivi l'un (1) des cours de formation suivants: 1) administrateur certifié de RSA Archer; 2) administrateur d'OpenPages d'IBM; 3) administrateur certifié en gestion d'administration de système de gouvernance, risque et conformité de Metricstream. Une copie du certificat de cours valide de la ressource proposée doit être jointe à la soumission.	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience de la production et de l'évaluation de produits livrables de C et A aux fins d'accréditation d'un système de TI.	Total:
$\overset{\circ}{\mathbf{Z}}$	C4	C5	

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)	
RÉFÉ PROP PARA	
NOTE	
MAX. DE POINTS	9
BARÈME DE NOTATION	Vivean 1 2 points = minimum d'expérience combinée démontrée avec deux (2) des solutions de sécurité des TI énumérées 3 points = minimum d'expérience combinée démontrée avec trois (3) des solutions de sécurité des TI énumérées 4 points = minimum d'expérience combinée démontrée avec quatre (4) des solutions de sécurité des TI énumérées 5 points = minimum d'expérience combinée démontrée avec cinq (5) des solutions de sécurité des TI énumérées 6 points = minimum d'expérience combinée démontrée avec au moins six (6) des solutions de sécurité des TI énumérées
N° CRITÈRES BAR	C.6 Ingenieur en sécurité des TII — Ni C1 Le soumissionnaire doit démontrer que la ressource proposée possède au moins une (1) année d'expérience combinée de l'élaboration et de la documentation de spécifications relatives aux exigences de système pour au moins deux (2) des solutions en matière de sécurité des TI suivantes : Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); Technologies de sécurité de réseautage sans fil; Systèmes de détection d'intrusion (IDS); Systèmes de prévention des intrusions dans un réseau (IPS); Gestion de l'information et des incidents de sécurité (SIEM); Saisie intégrale de paquet (FPC); Contrôle de l'accès au réseau (NAC); Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou
\mathbf{z}	C1 Per Signal Control

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)				
NOTE				
MAX. DE POINTS	3	3	3	Note maximale: 15 points
BARÈME DE NOTATION	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	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	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	Note de passage minimale : 8 points
N° CRITÈRES	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans le développement d'architectures de sécurité réseau (niveau II ou supérieur) basées sur les directives de sécurité des TI (DSTI) ou les conseils en matière de sécurité des TI (TSG).	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans la création ou la réalisation d'analyses de plans de continuité des activités et de reprise après sinistre.	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans la rédaction de rapports techniques comme des analyses des options ou des plans de mise en œuvre.	Total:
$\overset{\circ}{\mathbf{Z}}$	C2	C3	C4	

7
Niveau
I
\mathbf{II}
des
ij
sécurité
en
énieur
Ing
9
ن

°Z	N° CRITÈRES	BABEME DE NOTATION	MAX	NOTE	RÉFÉRENCE À LA
,			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.6 Ir	C.6 Ingénieur en sécurité des TI – Ni	iveau 2			
C1	Le soumissionnaire doit démontrer	1 point = minimum d'expérience	5		
	que la ressource proposée possède	combinée démontrée avec une (1) des			
	au moins deux (2) années	solutions de sécurité des TI			
	d'expérience combinée de	énumérées			
	l'élaboration et de la documentation	2 points = minimum d'expérience			
	de spécifications relatives aux	combinée démontrée avec deux (2)			
	exigences de système pour les	des solutions de sécurité des TI			
	solutions en matière de sécurité des	énumérées			
	TI suivantes:	3 points = minimum d'expérience			
		combinée démontrée avec trois (3)			
	Systèmes de prévention des	des solutions de sécurité des TI			
	intrusions au niveau de	énumérées			
	l'hôte (HIPS):	4 points = minimum d'expérience			
	H. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	combinée démontrée avec quetre (1)			
	I echnologies de securite de	combinee demondee avec quane (4)			
	réseautage sans fil;	des solutions de securité des 11			
	 Systèmes de détection 	énumérées			
	d'intrusion (IDS);	5 points = minimum d'expérience			
	 Systèmes de prévention des 	combinée démontrée avec au moins			
	intrusions dans un réseau	cinq (5) des solutions de sécurité des			
	(IPS);	TI énumérées			
	 Gestion de l'information et 				
	des incidents de sécurité				
	(SIEM);				
	 Saisie intégrale de paquet 				
	(FPC);				
	• Contrôle de l'accès au				
	réseau (NAC);				
	 Gestion de l'identité, des 				
	justificatifs d'identité et de				
	l'accès (ICAM); et/ou				
	 Protection des terminaux. 				

RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
NOTE						
MAX.	DE	POINTS	2	Note	maximale:	19 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale :	11 points	
N° CRITÈRES			missionnaire doit démontrer ressource proposée détient des certifications suivantes : tified Information System curity Professional (CISSP); tified Cloud Security ofessional (CSSP); et stems Security Certified ofessional (SSCP).	Total:		
$\overset{\circ}{\mathbf{Z}}$			S			

7	$\overline{}$	t
C	٧	7
_	`	È
•		j

RÉFÉRENCE À LA PROPOSITION (PAGE ET PARAGRAPHE)	
NOTE	
MAX. DE POINTS	2
veau 3 BARÈME DE NOTATION	1 point = minimum d'expérience combinée démontrée avec une (1) des solutions de sécurité des TI énumérées 2 points = minimum d'expérience combinée démontrée avec deux (2) des solutions de sécurité des TI énumérées 3 points = minimum d'expérience combinée démontrée avec trois (3) des solutions de sécurité des TI énumérées 4 points = minimum d'expérience combinée démontrée avec quatre (4) des solutions de sécurité des TI énumérées 5 points = minimum d'expérience combinée démontrée avec quatre (4) des solutions de sécurité des TI énumérées 5 points = minimum d'expérience combinée démontrée avec au moins cinq (5) des solutions de sécurité des TI énumérées
C.6 Ingenieur en securité des TI – Niveau 3 N° CRITÈRES BAR	Le soumissionnaire doit démontrer que la ressource proposée possède au moins quatre (4) années d'expérience combinée de l'élaboration et de la documentation de spécifications relatives aux exigences de système pour les solutions en matière de sécurité des TI suivantes: 1) Systèmes de prévention des intrusions au niveau de l'hôte (HIPS); 2) Technologies de sécurité de réseautage sans fil; 3) Systèmes de détection d'intrusion (IDS); 4) Systèmes de prévention des intrusions dans un réseau (IPS); 5) Gestion de l'information et des incidents de sécurité (SIEM); 6) Saisie intégrale de paquet (FPC); 7) Contrôle de l'accès au réseau (NAC); 8) Gestion de l'identité, des justificatifs d'identité et de l'accès (ICAM); et/ou
C.6 In N°	C.6.In

C2

u 3	
Nivea	
- 1	
\mathbf{II}	
des	
éd	
IŢ	
écur	
de s	
Ē	
conceptio	
ep	
nc	
5	
en	
ste	
alië	
éci	
\mathbf{Sp}	
C.7	
J	

;		H			
$\overset{\circ}{\mathbf{Z}}$	CRITERES	BAREME DE NOTATION	MAX.	NOTE	REFERENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.7S	C.7 Spécialiste en conception de sécu	nrité des TI – Niveau 3			
ū	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans la conception d'architectures sécurisées en respectant les lignes directrices des conseils en matière de sécurité des technologies de l'information du Centre de la sécurité des télécommunications.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
C3	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans l'analyse d'au moins un (1) des éléments suivants: 1) outils et techniques de sécurité des TI; 2) données de sécurité et présentation d'avis et de rapports; 3) statistiques sur la sécurité des 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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		
ຮ	Le soumissionnaire doit démontrer que la ressource proposée possède de l'expérience dans les études de classification ou de désignation du niveau de sécurité des données.	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 8 années d'expérience 4 points = plus de 8 années d'expérience	4		

\mathbf{Z}°	N° CRITÈRES	BARÈME DE NOTATION MAX. NOTE RÉFÉRENCE À LA	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
	Total:	Note de passage minimale :	Note		
		12 points	maximale:		
			20 points		

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

°Z	N° CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			DE		PROPOSITION (PAGE ET
			POINTS		PARAGRAPHE)
C.8 A	C.8 Analyste de la sécurité des réseaux – Niveau 3	ux – Niveau 3			
C1	Le soumissionnaire doit démontrer	2 points = minimum d'expérience	5		
	que la ressource proposée possède	combinée démontrée avec deux (2)			
	au moins trois (3) années	des solutions de sécurité des TI			
	d'expérience combinée dans	énumérées			
	l'examen, l'analyse, la mise en	3 points = minimum d'expérience			
	œuvre et l'appui d'au moins	combinée démontrée avec trois (3)			
	deux (2) des solutions en matière de	des solutions de sécurité des TI			
	sécurité suivantes :	énumérées			
		4 points = minimum d'expérience			
	1) protocoles de sécurité Internet;	combinée démontrée avec quatre (4)			
	2) protocoles réseau;	des solutions de sécurité des TI			
	3) algorithmes cryptographiques;	énumérées			
	4) normes d'annuaire;	5 points = minimum d'expérience			
	5) renforcement de la sécurité	combinée démontrée avec cinq (5)			
	réseau;	des solutions de sécurité des TI			
	6) systèmes d'exploitation.	énumérées			

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)																												
MAX. N	DE	POINTS	5																											
		PO	spérience	is trois (3)		spérience	s quatre (4)		spérience	is cing (5)																				
BARÈME DE NOTATION			3 points = minimum d'expérience	combinée démontrée dans trois (3)	des domaines énumérés	4 points = minimum d'expérience	combinée démontrée dans quatre (4)	des domaines énumérés	5 points = minimum d'expérience	combinée démontrée dans cinq (5)																				
CRITÈRES			Le soumissionnaire doit démontrer	que la ressource proposée possède	au moins deux (2) années	d'expérience dans l'élaboration	d'exigences et la conception	d'applications et d'infrastructures de	sécurité des TI dans au moins	trois (3) des domaines suivants :	1) Systèmes de prévention des	l'hôte (HIPS):	2) Technologies de sécurité de	-	3) Systèmes de détection	d'intrusion (IDS);	4) Systèmes de prévention des	intrusions dans un réseau	(IPS);	5) Gestion de l'information et	des incidents de sécurité	(SIEM);	6) Saisie intégrale de paquet	(FPC);	7) Contrôle de l'accès au	réseau (NAC);	8) Gestion de l'identité, des	justificatifs d'identité et de	l'accès (ICAM); et/ou	9) Protection des terminaux.
$\overset{\circ}{\mathbf{Z}}$			C2																											_

S.
\equiv
ea
.≥
Ź
$\overline{}$
_
\mathbf{I}
Ś
de
té
ırit
_
séc
de
_
3
E
tèmes
\mathbf{z}
S
de s
7
<u>-</u>
en
ate
ra
ě
C
$\overline{}$
Q
ت

RIT	CRITÈRES	BARÈME DE NOTATION	MAX.	NOTE	RÉFÉRENCE À LA
			POINTS		PROPOSITION (PAGE ET PARAGRAPHE)
ur d	Opérateur de systèmes de sécuri	ité des TI – Niveau 3			
missi	Le soumissionnaire doit démontrer	3 points = minimum d'expérience	9		
resso	que la ressource proposée possède	combinée démontrée avec trois (3)			
ns de	au moins deux (2) années	des solutions de sécurité des TI			
rienc	d'expérience combinée dans	énumérées			
en, l	l'examen, l'analyse, la mise en	4 points = minimum d'expérience			
ou l'	œuvre ou l'appui d'au moins	combinée démontrée avec quatre (4)			
) de	trois (3) des solutions ou plus en				
de ;	matière de sécurité des TI suivantes :	énumérées			
		5 points = minimum d'expérience			
Ω,	Systèmes de prévention des	combinée démontrée avec cinq (5)			
.=	intrusions au niveau de	des solutions de sécurité des TI			
Ξ	'hôte (HIPS);	énumérées			
H	Fechnologies de sécurité de	6 points = minimum d'expérience			
ŗ,	réseautage sans fil;	combinée démontrée avec au moins			
Š.	Systèmes de détection	six (6) des solutions de sécurité des			
Ġ	l'intrusion (IDS);	TI énumérées			
Ω.	Systèmes de prévention des				
ii.	ntrusions dans un réseau				
	(IPS);				
9	Gestion de l'information et				
ğ	les incidents de sécurité				
9	(SIEM);				
Š	Saisie intégrale de paquet				
<u>H</u>	(FPC);				
Ö	Contrôle de l'accès au				
ré	réseau (NAC);				
Ö	Gestion de l'identité, des				
jī.	ustificatifs d'identité et de				
	'accès (ICAM); et/ou				
9) Pr	Protection des terminaux				

NOTE RÉFÉRENCE À LA	PROPOSITION (PAGE ET	PARAGRAPHE)				
NOTE						
MAX.	DE	POINTS	2	Note	maximale:	8 points
BARÈME DE NOTATION			2 points = preuve d'au moins une des certifications énumérées	Note de passage minimale :	5 points	
N° CRITÈRES			nissionnaire doit démontrer essource proposée détient des certifications suivantes : etified Information System curity Professional (CISSP); ertified Cloud Security ofessional (CCSP); and/or systems Security Certified ofessional (SSCP).	Total:		
$\overset{\circ}{\mathbf{Z}}$			23			