DEMANDE DE PROPOSITIONS
SERVICES PROFESSIONNELS EN INFORMATIQUE CENTRÉS SUR LES TÂCHES
POUR
SERVICES PARTAGÉS CANADA

Demande de propositions (DDP)

MODIFICATION NO. 02

Cette modification n^{o} 2 de DDP est émise afin de :

1- Reporter d'une semaine la date de clôture de la DP afin de la faire passer au 24 septembre 2014.
2- Apporter des changements administratifs;
3- Fournir les réponses du Canada aux questions de l'industrie.

1. Sur la page couverture de la **DP**, **MODIFIER** la date de clôture de la DP comme suit :

SUPPRIMER : 17 septembre 2014

INSÉRER : 24 septembre 2014

2. Dans la Partie 3 « Instructions pour la préparation des soumissions », MODIFIER comme suit l'article 3.4 de la Section III : Attestations :

SUPPRIMER : L'article en entier.

3. Dans la Partie 4 « Procédures d'évaluation et méthode de sélection », MODIFIER comme suit l'article 4.1 « Procédures d'évaluation » :

SUPPRIMER : L'alinéa d) en entier.

4. Dans la Partie 6 « Clauses du contrat subséquent », MODIFIER comme suit l'article 6.2 « Procédures de demande et d'autorisation de tâches » :

SUPPRIMER : Le paragraphe 6.2.8 « Ressources approuvées » en entier.

5. Dans la Pièce jointe 1 de la Partie 4, MODIFIER comme suit l'article 3 « Critères obligatoires » :

SUPPRIMER : La colonne « Exigence obligatoire » pour le critère O1 et

INSÉRER : Ce qui suit à la place :

Le soumissionnaire doit démontrer qu'il possède une expérience contractuelle dans la fourniture de toutes les catégories de ressources suivantes, pour le nombre requis de jours facturables par catégorie.

Catégorie de personnel	**Nombre minimal requis de jours facturables**
Analyste des activités	**1 600**
Spécialiste en protection et en planification stratégique de la sécurité des TI	**1 000**

Spécialiste de la certification et de l'accréditation et des évaluations de la menace et des risques des TI	**1 800**
Spécialiste de la conception de la sécurité des TI	**2 000**
Spécialiste des analyses de vulnérabilité de la sécurité des TI	**600**
Spécialiste de la protection des renseignements personnels	**600**

Les soumissionnaires doivent remplir les appendices A et B de la partie 4.

Les services fournis doivent l'avoir été dans le cadre de cinq contrats, tout au plus. Il n'est pas nécessaire que chacun des contrats vise toutes les catégories de personnel. Les contrats cités en référence doivent être d'une valeur excédentaire (« facturée ») de plus de 1 M$.

L'expérience doit avoir été acquise au cours des cinq années précédant la date de clôture de la demande de propositions. L'expérience peut avoir été obtenue à tout moment pendant la période de cinq ans, pourvu que le nombre total de jours facturables, une fois additionnés, corresponde au nombre minimal requis de jours facturables.

Les travaux effectués par la catégorie de personnel doivent comprendre au moins 70 % des tâches connexes énumérées dans l'énoncé des travaux de la présente demande de soumissions pour cette catégorie de personnel.

5. Dans la Pièce jointe 1 de la Partie 4, MODIFIER comme suit l'article 4 « Critères techniques cotés» :

SUPPRIMER : La colonne « Critères d'évaluation cotés» pour le critère C1 et

INSÉRER : Ce qui suit à la place :

Le soumissionnaire devrait démontrer le nombre de jours d'expérience facturables qu'il a acquise en sus du minimum de jours facturables indiqués pour le critère O1.

Le nombre « total de jours facturables » indiqué par le soumissionnaire dans sa réponse au critère O1 servira à évaluer le présent critère.

Exemple de scénario d'évaluation

	JOURS facturables			
	(A)	(B)	(C)	(D)
CATÉGORIE DE PERSONNEL	N^{BRE} TOTAL DE JOURS FACTURABLES INDIQUÉ PAR LE SOUMISSIONNAIRE	N^{BRE} MINIMAL DE JOURS REQUIS POUR LE CRITÈRE O1	N^{BRE} DE JOURS EXCÉDENTAIRES	POURCENTAGE D'AUGMENTATION PAR RAPPORT AU N^{BRE} DE POINTS MAXIMUM (100 POINTS)
Analyste des activités	2 175	1 600	575	35,94
Spécialiste en protection et en planification stratégique de la	1 225	1 000	225	22,5

sécurité des TI				
Spécialiste de la certification et de l'accréditation et des évaluations de la menace et des risques des TI	4 000	1 800	2 200	100,00
Spécialiste de la conception de la sécurité des TI	3 000	2 200	800	36,36
Spécialiste des analyses de vulnérabilité de la sécurité des TI	850	600	250	41,67
Spécialiste de la protection des renseignements personnels	800	600	200	33,33
NOTE DU SOUMISSIONNAIRE = SOMME (D)/N^{BRE} DE CATÉGORIES				
Somme (D)/ 6 = 44,97				

On accordera des points au soumissionnaire pour le nombre de jours en sus du nombre minimal indiqué au critère O1, comme le montre l'exemple de scénario d'évaluation ci-dessous. Dans cet exemple, le soumissionnaire obtiendrait 44,97 points sur 100.

Les soumissionnaires doivent remplir les appendices A et B de la partie 4.

6. MODIFIER comme suit l'Appendice A de la Pièce jointe 1 de la Partie 4 « Critères d'évaluation » :

SUPPRIMER : La version précédente dans son intégralité.

INSÉRER : La nouvelle version qui est jointe à la présente modification de la demande de propositions.

7. MODIFIER comme suit la Pièce jointe 2 de la Partie 4 « Évaluation financière de la proposition (tableau des prix) » :

SUPPRIMER : La version précédente dans son intégralité.

INSÉRER : La nouvelle version qui est jointe à la présente modification de la demande de propositions.

8. MODIFIER l'Annexe A « Énoncé des travaux » comme suit :

SUPPRIMER : La version précédente dans son intégralité.

INSÉRER : La nouvelle version qui est jointe à la présente modification de la demande de propositions.

9. Fournir les réponses du Canada aux questions de l'industrie reçues pendant la question période

Question	Réponse
8- L'Appendice B de la Partie 4 exige les coordonnées de la personne référence d'un client en particulier. Du fait de la nature des travaux liés à la sécurité, nos contrats et nos règles d'engagement requièrent la confidentialité et nous ne sommes pas autorisés à divulguer les noms des clients. Comme pour d'autres de ses soumissions, SPC accepte-t-il que les soumissionnaires ajoutent la mention « Confidentiel » lorsque l'organisation et les coordonnées du client doivent demeurer confidentielles, pourvu qu'ils FOURNISSENT le nom de l'organisation et autres coordonnées directement à SPC dans les 24 heures suivant la demande?	SPC accepte que les soumissionnaires ajoutent la mention « Confidentiel » lorsque l'organisation et les coordonnées du client doivent demeurer confidentielles, pourvu qu'ils FOURNISSENT le nom de l'organisation et autres coordonnées directement à SPC dans les 24 heures suivant la demande.
9- Question concernant le rôle des petites entreprises dans les contrats de services professionnels de Services partagés Canada (SPC). La demande de proposition (DP) 13-18801-0/A est une DP de grande envergure, s'étendant sur plusieurs années et faisant appel à de nombreuses ressources. Elle comprend 6 fonctions de sécurité des TI et 72 ressources dans le cadre des mécanismes de passation de marchés (non réservés aux entreprises autochtones) des Services professionnels en informatique centrés sur les tâches (SPICT). Dans ce contrat, les exigences obligatoires touchant l'organisation sont visiblement adaptées aux très grandes organisations et visent à exclure les petites et moyennes entreprises. De plus, les exigences sont expressément rédigées d'une manière qui vise à empêcher les fournisseurs de petite et moyenne taille de former des coentreprises de deux entreprises ou plus. Cette intention est visible par l'utilisation d'une seule exigence obligatoire de l'organisation qui regroupe : ○ une expérience contractuelle de 5 millions de dollars; ○ 6 catégories de ressources; ○ une expérience de 7 600 jours facturables (plus de 33 années facturables). Cette combinaison habile empêche les petites et moyennes entreprises qui souhaiteraient former une coentreprise de mettre en commun leurs expériences contractuelles, leurs ressources ou leurs jours facturables et élimine efficacement ces fournisseurs de la compétition. La DP mentionne clairement (exigence cotée de l'organisation C2) que « Services partagés Canada	a) SPC continue d'effectuer des appels d'offres pour les volets 1 et 2 et d'attribuer des contrats pour ces volets afin de s'acquitter de son mandat. b) Seules les entités d'une coentreprise existante et officielle fournissant des services du volet 2 des SPICT sont autorisées à soumissionner; SPC ne reconnaîtra pas l'expérience énoncée par tout autre type de partenariats relativement aux exigences d'entreprise obligatoires et cotées.

(SPC) estime que le risque le plus important associé au contrat est l'incapacité de l'entrepreneur à fournir le nombre requis de ressources qualifiées, des catégories et du niveau exigés, dans les délais indiqués dans la demande de tâches ». La décision de combiner les exigences de l'organisation comme ci-dessus canaliserait toutes les possibilités vers une (et jusqu'à quatre, mais nous ne croyons pas qu'il y aura quatre soumissions conformes) grande entreprise. Or, les grandes entreprises n'ont pas le monopole des consultants expérimentés en sécurité des TI dans la région de la capitale nationale (RCN), et l'approche de SPC a pour effet de limiter son accès à du personnel qualifié. Nous sommes très préoccupés par le fait que cette DP soit réservée aux très grandes entreprises. Bien que l'efficacité et l'économie fassent partie du mandat de SPC et que son approche jusqu'à présent ait été de regrouper ses marchés auprès des très grandes entreprises, l'exclusion explicite des petites et moyennes entreprises des contrats de SPC causera des dommages irréparables à ces entreprises et à leur personnel. À l'extrême, en leur refusant l'accès aux mécanismes de passation de marchés du gouvernement du Canada auxquels elles pouvaient auparavant participer par divers instruments, ce désavantage pourrait provoquer la disparition d'entreprises spécialisées dans ce domaine. La DP stipule que « SPC peut décider de se servir du présent contrat pour une partie ou la totalité de ses clients et peut utiliser d'autres moyens pour prêter des services identiques ou semblables », mais on n'y trouve aucune précision ni aucun engagement à propos de ces autres moyens. Compte tenu de ce qui précède, veuillez : a) décrire les plans et échéanciers de SPC en ce qui concerne l'établissement d'instruments contractuels accessibles aux petites et moyennes entreprises; b) préciser si les exigences obligatoires et cotées de l'organisation peuvent être divisées de manière à permettre à de petites et moyennes entreprises de former une coentreprise pour ce contrat particulier.	

10- Question concernant le rôle des entreprises autochtones dans les contrats de services professionnels de Services partagés Canada (SPC). En réponse aux désavantages historiques vécus par les Autochtones canadiens, Travaux publics et Services gouvernementaux Canada (TPSGC), au nom du gouvernement du Canada, a mis en place des programmes pour soutenir les entreprises et les peuples autochtones qui souhaitent offrir leurs services au gouvernement. Ces programmes comprennent des stratégies d'approvisionnement réservé aux entreprises autochtones (REA) qui permettent aux entreprises autochtones de se développer et de croître dans un contexte concurrentiel. La plupart des offres à commande et des arrangements en matière d'approvisionnement de grande envergure gérés par TPSGC au cours des 10 dernières années, si ce n'est tous, comportaient ou comportent actuellement un volet REA. Citons, par exemple, les services de protection de la sécurité de l'infrastructure de la technologie de l'information (SPSITI), les arrangements en matière d'approvisionnement en cyberprotection (AMAC), les services professionnels en informatique centrés sur les solutions (SPICS) et les services professionnels en informatique centrés sur les tâches (SPICT). Les arrangements en matière d'approvisionnement d'envergure touchant le matériel et les logiciels, comme les services de soutien de l'équipement de réseau (SSER) et les arrangements en matière d'approvisionnement portant sur l'achat de licences de logiciels (AAALL), comportent eux aussi un volet REA. La demande de proposition (DP) 13-18801-0/A est une DP de grande envergure, s'étendant sur plusieurs années et faisant appel à de nombreuses ressources. Elle comprend 6 fonctions de sécurité des TI et 72 ressources dans le cadre des mécanismes de passation de marchés (non réservés aux entreprises autochtones) des Services professionnels en informatique centrés sur les tâches (SPICT). Les documents de la DP précisent que ce contrat sera utilisé « par SPC afin d'offrir des services partagés à ses clients, notamment à SPC lui-même, aux institutions gouvernementales pour lesquelles ses services sont obligatoires à un moment donné pendant la durée du contrat, et aux autres organisations pour	a) SPC continue de respecter les dispositions sur les entreprises autochtones de la Politique sur les marchés du Conseil du Trésor et s'efforce de conclure des marchés réservés aux entreprises autochtones dans la mesure du possible. b) Aucune composante liée aux marchés réservés aux entreprises autochtones n'est associée à cette exigence en particulier.

lesquelles les services de SPC sont facultatifs à un moment donné pendant la durée du contrat et qui choisissent d'y avoir recours de temps à autre ». Il est clair que l'intention de SPC est d'utiliser ce contrat comme une sorte d'arrangement en matière d'approvisionnement pour satisfaire à un grand nombre de besoins. Dans les faits, les entreprises autochtones incapables de se qualifier pour le contrat non REA se verront refuser la possibilité de fournir des services de sécurité des TI directement au plus grand consommateur de ces services au sein du gouvernement. L'absence de volet REA dans la présente DP nous préoccupe grandement. Bien que l'efficacité et l'économie fassent partie du mandat de SPC et que son approche jusqu'à présent ait été de regrouper ses marchés auprès des très grandes entreprises, le fait de ne pas créer ou inclure une stratégie d'approvisionnement auprès des entreprises autochtones au sein de SPC non seulement va à l'encontre de la position du gouvernement du Canada relativement aux marchés réservés aux entreprises autochtones, mais risque de causer des dommages irréparables aux entreprises et aux ressources autochtones dans le domaine de la sécurité des TI dans la capitale nationale. À l'extrême, en refusant aux entreprises autochtones l'accès aux mécanismes de passation de marchés du gouvernement du Canada auxquels elles pouvaient auparavant participer au moyen des marchés réservés aux entreprises autochtones, ce désavantage pourrait provoquer la disparition d'entreprises autochtones dans ce domaine. La DP stipule que « SPC peut décider de se servir du présent contrat pour une partie ou la totalité de ses clients et peut utiliser d'autres moyens pour prêter des services identiques ou semblables », mais on n'y trouve aucune précision ni aucun engagement à propos de ces autres moyens. Compte tenu de ce qui précède, veuillez : 1. décrire les plans et échéanciers de SPC en ce qui concerne l'établissement de marchés réservés aux entreprises autochtones; 2. préciser s'il y aura un volet REA pour ce contrat particulier.	
11- Y a-t-il actuellement (ou y a-t-il déjà eu) un expert-conseil assurant la prestation de services semblables ou identiques à ceux demandés aux présentes? Si tel est le cas, quelle est la société	Au cours des 12 derniers mois, pour la CSTI (cybersécurité et sécurité de la TI), on a utilisé un certain nombre de mécanismes SPICT pour se procurer des ressources similaires dans le cadre

contractante et quelle est (ou quelle était) la valeur du contrat?	d'autorisations de tâches individuelles, à savoir les SIST (services d'ingénierie et de soutien technique et les SPOT (services professionnels opérationnels et technologiques) Les entreprises titulaires comprennent CGI pour le mécanisme SIST qui prend fin le 31 octobre 2014. Pour le mécanisme SPOT, les entreprises titulaires comprennent Eagle, TEK Systems et Maplesoft. Chacun de ces fournisseurs a, à l'occasion, fourni diverses ressources pour des durées de contrats initiaux de six mois avec options de prolongation. Il est estimé qu'environ 7,5 M$ ont été consacrés à des services professionnels en CSTI par l'intermédiaire de ces mécanismes.
12- Nous avons une question pour l'État en ce qui concerne la demande de propositions 13-18801-0/A - Ressources pour la transformation de la cybersécurité et de la sécurité des TI. Y a-t-il en ce moment, ou y a-t-il déjà eu, un ou plusieurs consultants offrants des services semblables ou identiques à ceux demandés ici? Le cas échéant, quelle est ou était l'entreprise contractante et quelle est ou était la valeur du contrat? Nous avons examiné la présente DP et déterminé que, compte tenu de l'ampleur des exigences de l'organisation pour ces services professionnels en informatique centrés sur les tâches (SPICT), nous (et plusieurs autres) n'étions pas en mesure de soumissionner. Nous demeurons cependant perplexe quant aux raisons pour lesquelles des membres de l'industrie qui se sont donné beaucoup de mal pour se qualifier pour le volet 2 de ces SPICT se voient empêchés de présenter une soumission à cause de l'imposition par l'État d'exigences obligatoires touchant l'organisation supplémentaires. De plus, nous nous sommes donné la peine de faire équipe (comme entrepreneur principal ou sous-traitant) avec d'autres membres de l'industrie et avons constaté que plusieurs autres entreprises ne peuvent elles non plus satisfaire à ces exigences obligatoires supplémentaires non nécessaires touchant	a) L'État se réserve le droit d'inclure des exigences d'entreprise supplémentaires afin de servir ses intérêts supérieurs. b) SPC ne retirera pas la DP pour des SPICT.

l'organisation. Ces exigences ne servent qu'à restreindre la concurrence, à protéger les entrepreneurs titulaires des contrats actuels et à augmenter considérablement les coûts du contrat pour l'État. L'État pourrait-il envisager d'éliminer les exigences de l'organisation? Dans le cas contraire, dans l'intérêt d'un processus d'approvisionnement fiscalement responsable, l'État pourrait-il envisager d'annuler ces SPICT et de tout simplement lancer cette DP comme s'il s'agissait de son propre contrat, ce qui permettrait aux entreprises de créer des coentreprises? Les soumissions de coentreprises ne sont pas autorisées dans le cadre des SPICS, à moins qu'elles aient été le moyen utilisé au départ pour se qualifier pour le volet. Comme beaucoup d'autres, nous n'avions pas besoin d'une coentreprise pour nous qualifier pour le volet 2, mais comme nous l'avons expliqué, nous ne pouvons satisfaire à cette exigence.	
13- En ce qui concerne l'exigence obligatoire qui consiste à démontrer que l'ouvrage livré par la catégorie de personnel doit comprendre au moins 70 % des tâches connexes qui sont énumérées dans l'énoncé des travaux, SPC peut-il confirmer que cette proportion de 70 % concerne les tâches précédées d'une puce et non les qualificatifs précédés d'une lettre (soit les points accompagnés des lettres a), b), etc. qui suivent certaines des tâches précédées d'une puce?	Pour justifier chaque catégorie de personnel, les soumissionnaires doivent démontrer que les projets cités en référence abordent au moins 70 % des éléments liés aux tâches. Lorsqu'un élément comprend une liste de sous-tâches (c.-à-d. points a à g), le projet cité en référence doit aborder au moins 70 % des sous-tâches pour que l'élément soit considéré comme justifié.
14- En raison des nombreux processus d'approvisionnement de services professionnels en cours et d'autres programmes de TI dont la réponse à l'appel d'offres demande plusieurs hommes-heures de la part du même bassin d'experts, nous demandons respectueusement une prolongation d'un mois, soit jusqu'au 17 octobre 2014. Nous demandons également que la période de questions soit prolongée jusqu'au 3 octobre 2014.	La date de clôture est reportée au 24 septembre 2014 à 14 h, heure avancée de l'Est (HAE).
15- Page 3 de 93, clause 1.2 « Résumé ». Veuillez confirmer que l'entente de non-divulgation signée ne doit être fournie qu'après l'attribution du contrat.	Nous le confirmons.

16- Page 12 de 93, clause 4.1 « Procédures d'évaluation », point d) : « Le soumissionnaire doit inclure un curriculum vitæ à jour pour la ressource proposée » : Veuillez confirmer que cela ne sera exigé qu'au moment de l'autorisation de tâches.	Le point d) du paragraphe 4.1 de la Partie 4 renvoie à la demande de tâches après l'attribution du contrat; il ne doit donc pas être supprimé.
17- Page 20 de 93, clause 5.1 « Exigences obligatoires au moment de l'attribution du contrat – Exigences relatives à la sécurité » : Veuillez confirmer que l'attestation de sécurité n'est exigée qu'au moment de l'autorisation de tâches.	Les entrepreneurs doivent détenir une attestation de sécurité au moment de la demande de tâches.
18- À la page 29 de 93, le point i. de la clause 6.2.8 « Ressources approuvées » énonce ce qui suit : « s'assurer que les personnes nommées à l'Annexe E de ce contrat [...] ». Veuillez confirmer que l'Annexe E est manquante ou non requise et que les noms des ressources ne devront être fournis qu'au moment de l'autorisation de tâches.	L'Annexe E n'est pas requise dans le cadre de la présente DP et sera supprimée au moyen d'une modification à la DP.
19- L'exigence obligatoire O1 de la page 83 de 93 énonce ce qui suit : « Les soumissionnaires doivent remplir les appendices A, B et C de la partie 4 ». SPC pourrait-il clarifier ce que constitue l'Appendice C ou supprimer la mention de cette dernière?	L'Annexe C n'existe pas et cette référence a été supprimée.
20- Pour ce qui est de l'exigence cotée C2 de la page 84 de 93, veuillez confirmer que le deuxième paragraphe, « Le fournisseur devrait démontrer sa capacité à fournir [...] de grands groupes de ressources à l'appui d'un seul client ou projet [...] », signifie que tout service professionnel (c.-à-d. ce qui ne touche pas la cybersécurité et la sécurité de la TI) répond aux critères de référence.	Nous le confirmons.
21- Pour ce qui est du deuxième paragraphe de la Pièce jointe 2 de la Partie 4, « Évaluation financière », à la page 87 de 93, veuillez confirmer que la phrase « Il doit proposer le même tarif journalier pour tous les employés » est une erreur et qu'elle devrait être supprimée.	Nous le confirmons.
22- Veuillez confirmer que dans l'Appendice A de la Pièce jointe 1 la mention « Période de facturation (24 mois consécutifs) » devrait être remplacée par « Période de facturation (60 mois consécutifs) ».	Nous le confirmons.
23- Puisque la page couverture qui renferme des renseignements essentiels à la préparation et la présentation d'une offre a été remise 15 jours après la publication de la DDP et puisque l'appendice C à la partie 4 ne se trouve pas dans le dossier de DDP, laquelle constitue un autre document obligatoire et nécessaire afin de pouvoir	La date de clôture est reportée au 24 septembre 2014 à 14 h, heure avancée de l'Est (HAE).

évaluer, préparer et soumettre une offre, nous demandons à l'État de reporter la date d'échéance de remise des offres de 15 jours, soit jusqu'au 2 octobre 2014 à 14 h.	
24- Dans la demande de propositions 13-18801/A, il est indiqué qu'un maximum de quatre (4) contrats sera attribué par suite de cette demande. Est-ce à dire que les soumissionnaires peuvent présenter une proposition qui ne contiendrait pas toutes les catégories de personnel énumérées dans la demande de soumissions?	Non.
25- L'État peut-il confirmer que les soumissionnaires peuvent ne présenter qu'une (1) seule ressource admissible pour chaque catégorie de personnel?	À l'aide des projets cités en référence, les soumissionnaires doivent démontrer le nombre minimal de jours facturables et aborder au moins 70 % des tâches énumérées pour chaque catégorie de personnel. Les soumissionnaires peuvent se servir de l'expérience acquise par un nombre de ressources affectées au projet, à condition que leurs tâches dans le cadre du projet respectent les critères. Ce n'est toutefois qu'après l'attribution du contrat, pendant une demande de tâches, que les ressources particulières seront évaluées en fonction d'une grille d'évaluation des ressources préparée.
26- L'État étudiera-t-il la possibilité de permettre aux entreprises de continuer à démontrer tous les services pertinents qu'elles ont offerts dans le cadre de cinq contrats au cours des cinq dernières années, tout en cotant les totaux, plutôt qu'en imposant un minimum obligatoire?	Les jours facturables obligatoires et les jours facturables cotés demeurent inchangés.
27- L'État peut-il indiquer combien ont été attribués de contrats concernant des évaluations des facteurs relatifs à la vie privée ayant nécessité un niveau d'effort de plus de 120 jours (600/5)?	Les valeurs obtenues pour le critère O1, le critère C1 et le nombre total estimé de ressources requises (par année) sont fondées sur des modèles opérationnels actuels et des prévisions établies en fonction du mandat et des priorités de SPC et du Programme de transformation de la cybersécurité et de la sécurité de la TI.
28- L'État accepte-t-il que nous remontions jusqu'à huit ans pour ce qui est du niveau d'effort?	Non.
29- Puisque SPC a publié au moins trois demandes de soumissions dont l'échéance est la même, cela a entraîné un fardeau considérable pour les entreprises qui se sont qualifiées et qui souhaitent présenter des offres dans le cadre de plus d'une demande. Puisque la plupart des entreprises doivent souvent présenter plusieurs offres dans l'espoir d'être sélectionnées. Pour ces raisons, nous demandons respectueusement que soit reportée de 10 jours civils la date de clôture actuelle.	La date de clôture est reportée au 24 septembre 2014 à 14 h, heure avancée de l'Est (HAE).

30- Étant donné que la page couverture, qui contient des renseignements essentiels pour la préparation et la présentation d'une soumission, a été fournie 15 jours après la publication de la demande de propositions et du fait que l'Appendice C de la Partie 4 ne figure pas dans la trousse de demande de propositions, là aussi un document dont nous avons besoin pour évaluer la demande de propositions, puis pour préparer et présenter notre soumission, nous demandons à l'État de prolonger le délai de 15 jours, soit jusqu'au 2 octobre 2014, à 14 h.	La date de clôture est reportée au 24 septembre 2014 à 14 h, heure avancée de l'Est (HAE).
31- Il est évident que l'État s'en remet au critère obligatoire (M1) pour qualifier les organisations de sécurité qui ont démontré sans l'ombre d'un doute qu'elles possédaient l'expérience et l'expertise nécessaires en fournissant depuis longtemps des ressources en matière de sécurité à des organisations canadiennes. La constriction de : • Les catégories exactes • Pour le nombre exact de journées facturables (7 600 en tout, soit 34,55 années d'expérience) • Dans le cadre d'au plus cinq contrats • Ces contrats doivent avoir été réalisés au cours des cinq dernières années • La valeur facturée des contrats doit atteindre au moins 1 million de dollars Il n'est pas pratique de demander 34,55 années d'expérience dans les catégories précises sur une période de 5 ans pour un contrat d'un an plus deux années d'option, puisque cela limitera le nombre d'offres de qualité que SPC recevra, sans compter qu'on pourrait juger qu'un tel processus favorise les organisations titulaires. Le réseau que gère SPC pour le gouvernement du Canada est le plus important consommateur d'experts-conseils et de services dans le domaine de la sécurité au pays. Par conséquent, en exigeant un minimum de 34 années d'expérience pour se qualifier, on limite sérieusement le nombre d'entreprises de	Les exigences relatives aux services professionnels auxquelles ce critère vise à répondre sont axées sur les tâches. Pour les approvisionnements du volet 2, SPC évalue souvent l'expérience en jours facturables des soumissionnaires selon des catégories de personnel pertinentes, y compris leur description. Considérant une expérience de 220 jours facturables par année pour une période de 5 ans, SPC attribuera tous les points aux soumissionnaires qui démontrent une expérience équivalente pour 3 analystes des activités (3 200 jours), 2 spécialistes en protection et en planification stratégique de la sécurité des TI (2 000 jours), 3,5 spécialistes de la certification et de l'accréditation et des évaluations de la menace et des risques des TI (3 600 jours), 4 spécialistes de la conception de la sécurité des TI (4 000 jours), 1,1 spécialiste des analyses de vulnérabilité de la sécurité des TI (1 200 jours) et 1,1 spécialiste de la protection des renseignements personnels (1 200 jours). Les projets de référence des clients ne se limitent pas à ceux du gouvernement du Canada. Conformément à la modification nº 1, un seul contrat conclu avec l'Agence de la fonction publique du Canada peut être utilisé pour répondre aux critères O1 et C1. Aucun autre changement ne sera envisagé.

sécurité très compétentes et matures qui seront en mesure de présenter des offres. Il n'est pas habituel que les contrats de sécurité au Canada soient aussi longs ou qu'ils présentent une valeur aussi élevée que celle que le Canada demande dans cet appel d'offres. Il est habituel qu'une organisation importante dans le domaine de la sécurité dispose d'une pratique prospère répartie sur plusieurs contrats de moindre envergure afin de consolider les réseaux qu'elle protège. Compte tenu de la structure du contrat que l'État semble privilégier, plusieurs organisations qualifiées (au plus 4) se livreront concurrence au fur et à mesure des besoins. Par conséquent, dans le but de préserver l'intégrité du processus d'approvisionnement et présenter à SPC le nombre maximal de soumissionnaires qualifiés dans le domaine de la sécurité qui ont fait la preuve d'une pratique mature à ce niveau et qui sont plus qu'en mesure de fournir des ressources qualifiées à SPC, nous demandons à l'État de revoir le critère obligatoire 1 afin qu'il se lise comme suit : ***Le soumissionnaire devrait démontrer qu'il possède une expérience récente suffisante dans la prestation de services de consultation sur la sécurité des TI. Pour démontrer cette expérience, le soumissionnaire doit avoir facturé des services de consultation sur la sécurité des TI pour un montant d'au moins 5 000 000 $. Seul le travail facturé depuis le 17 septembre 2009 sera accepté.*** ***Les renseignements suivants doivent être fournis afin de corroborer le volume d'affaires allégué :*** ***- Numéros des contrats*** ***- Noms et coordonnées des clients à des fins de vérification*** ***- Dates de début et de fin des contrats, incluant les périodes d'option*** ***- Montants des contrats*** ***- Montant facturé pour chaque contrat cité en référence*** ***- Description des services rendus***	

Les services de consultation sur la sécurité des TI se définissent comme étant l'équivalent des activités communes des catégories de ressources en vertu des catégories de SPICT énumérées dans l'arrangement en matière d'approvisionnement. ***Le soumissionnaire doit avoir fourni des services à des clients de l'extérieur. Les « clients de l'extérieur » se définissent comme des entités juridiques qui ne sont pas des sociétés apparentées, des filiales ou des sociétés affiliées du soumissionnaire. Cela concerne tous les membres d'une coentreprise qui présentent une offre.***	
32- Dans le critère C1, qui constitue la suite de M1, on demanderait 34,55 années (ou 7 600 jours) d'expérience additionnelle pour obtenir le maximum de 100 points; soit un total de 15 200 jours ou 69,1 ans au moment de combiner les critères M1 et C1. Compte tenu du contexte de la sécurité au Canada, cette demande ne semble pas réaliste ou conforme au désir de SPC d'accorder jusqu'à quatre contrats de services de sécurité au fur et à mesure de ses besoins. Comme nous l'avons mentionné dans notre question ci-dessus (pour le critère M1), le critère C1, tel qu'il est actuellement formulé, limiterait le nombre d'offres qualifiées que SPC recevra, de sorte que nous demandons de modifier le critère C2 afin qu'il se lise comme suit : ***Le soumissionnaire devrait démontrer qu'il possède une expérience récente suffisante dans la prestation de services de consultation sur la sécurité des TI. Pour faire la démonstration d'une telle expérience, le soumissionnaire doit dresser la liste des recettes facturées tirées des services de consultation sur la sécurité des TI qu'il a dispensés jusqu'à un montant de 10 millions $ en sus du critère M1 afin d'obtenir la totalité des points. Seul le travail facturé depuis le 17 septembre 2009 sera accepté.*** ***Les renseignements suivants doivent être fournis afin de corroborer le volume d'affaires allégué :*** ***- Numéros des contrats*** ***- Noms et coordonnées des clients à des fins de vérification***	Veuillez consulter la réponse à la question 31.

- Dates de début et de fin des contrats, incluant les périodes d'option ***- Montants des contrats*** ***- Montant facturé pour chaque contrat cité en référence*** ***- Description des services rendus*** ***Les services de consultation sur la sécurité des TI se définissent comme étant l'équivalent des activités communes des catégories de ressources en vertu des catégories de SPICT énumérées dans l'arrangement en matière d'approvisionnement.*** ***Le soumissionnaire doit avoir fourni des services à des clients de l'extérieur. Les « clients de l'extérieur » se définissent comme des entités juridiques qui ne sont pas des sociétés apparentées, des filiales ou des sociétés affiliées du soumissionnaire. Cela concerne tous les membres d'une coentreprise qui présentent une offre.*** • **De 5 M $ à 6 M $ = 20 points** • **Plus de 6 M $ à 7 M $ = 40 points** • **Plus de 7 M $ à 8 M $ = 60 points** • **Plus de 8 M $ à 9 M $ = 80 points** • **Plus de 9 M $ à 10 M $ = 100 points**	
33 Comme l'indique le critère C2, SPC a raison de croire que le risque le plus important que présente ce contrat concerne la capacité d'un entrepreneur de fournir le nombre exigé de ressources qualifiées. Cependant, il n'est pas réaliste de valider la capacité des éventuels entrepreneurs de fournir un volume élevé de ressources dans le cadre d'un seul contrat dans la RCN au cours des 12 à 24 derniers mois. Les contrats actuels de SPC représentent probablement les seules ententes qui permettraient d'obtenir tous les points, ce qui, par conséquent, limite le nombre d'offres que SPC recevra. Il est évident que SPC souhaite que les organisations fassent la preuve qu'elles disposent d'un effectif de réserve et, pour cette raison, nous	Compte tenu du processus de répartition des tâches et du volume potentiel d'autorisations de tâches visé par un contrat attribué dans le cadre de la présente demande de soumissions, il est essentiel que les soumissionnaires retenus aient déjà de l'expérience dans la prestation de services à volume élevé à un client de la région de la capitale nationale. Le client de référence ne se limite pas au gouvernement du Canada. Aucun changement au critère C2 ne sera envisagé.

demandons qu'on modifie le critère C2 afin qu'il se lise comme suit : **Services partagés Canada (SPC) estime que le risque le plus important associé au contrat est l'incapacité de l'entrepreneur à fournir le nombre requis de ressources qualifiées, des catégories et du niveau exigés, dans les délais indiqués dans la demande de tâches.** **Le fournisseur devrait démontrer sa capacité à fournir, à gérer et à maintenir de grands groupes de ressources à l'appui des projets des clients dans la région où les travaux sont réalisés** **Le soumissionnaire devrait fournir une liste des contrats réalisés pour des clients et citer en référence un minimum de dix personnes ressources ayant travaillé, au cours des 12 à 24 derniers mois, dans la région de la capitale nationale à l'appui des projets des clients.** **Pour qu'elle soit prise en compte, une ressource donnée ne peut être utilisée/comptée qu'une seule fois.** **Le projet cité en référence doit comprendre les renseignements suivants :** • **Nom de l'organisation cliente** • **Nom et titre de la personne-ressource du client** • **Numéro de téléphone de la personne-ressource du client** • **Adresse de courriel de la personne-ressource du client** • **Dates de début et de fin du projet (aa/mm)** • **Nombre total de ressources des Services professionnels fournies au cours des 12 à 24 derniers moins** • **10 points**- 10 ressources individuelles ont été fournies à des clients dans la RCN au cours des 12 à 24 derniers mois; • **25** points- 15 ressources individuelles ont été fournies à des clients dans la RCN au cours des 12 à 24 derniers mois; • **35** points- 25 ressources individuelles ont été fournies à des clients dans la RCN au cours des 12 à 24 derniers mois; **50** points- 30 ressources individuelles ont été	

fournies à des clients dans la RCN au cours des 12 à 24 derniers mois.	
34- Veuillez fournir l'appendice C de la partie 4 de la DDP, puisqu'elle ne se trouve pas dans le dossier de DDP et parce qu'elle est nécessaire pour évaluer, préparer et soumettre une offre dans le cadre de cette demande de soumissions. Puisqu'il manque de l'information et dans le but de protéger l'intégrité du processus d'appel d'offres, ainsi que pour garantir que SPC recevra un nombre maximal d'offres qu'il faudra évaluer, nous demandons que soit accordée une prolongation jusqu'au 2 octobre 2014.	L'Annexe C n'est pas obligatoire pour présenter des soumissions dans le cadre de la présente demande de propositions. Par conséquent, elle a été supprimée. Cela ne justifie pas une prolongation.
35- Le critère obligatoire O1 exige que les soumissionnaires remplissent l'Appendice A de la Partie 4 pour justifier leur expérience et que l'expérience servant à démontrer les jours facturables ait « été acquise au cours des cinq années précédant la date de clôture de la demande de propositions. L'expérience peut avoir été obtenue à tout moment pendant la période de cinq ans, pourvu que le nombre total de jours facturables, une fois additionnés, corresponde au nombre minimal requis de jours facturables ».	La période de 24 mois est incorrecte. Cette période est de 60 mois. Cette erreur a été corrigée dans la modification à la demande de propositions. Compte tenu du report de la date de clôture des soumissions, le soumissionnaire aura plus de temps pour poser des questions au sujet de la demande de propositions.
36- L'État envisagera-t-il de permettre aux entreprises de faire quand même la démonstration de tous les services pertinents qu'ils ont offerts dans le cadre de cinq contrats réalisés au cours des cinq dernières années en permettant de coter les totaux plutôt qu'un minimum obligatoire?	Aucun changement relatif au nombre de contrats requis pour démontrer une expérience suffisante ne sera envisagé.

TOUTES LES AUTRES MODALITÉS DE CETTE INVITATION À SE QUALIFIER DEMEURENT INCHANGÉES.

==========

Un résumé des modifications à la Demande de propositions (DDP) émises jusqu'à ce jour figure ci-dessous.

Suivi des documents	Date	Description
Modification nº 001	28 août 2014	Apporter des changements administratifs et fournir les réponses du Canada aux questions de l'industrie
Modification nº 002	08 septembre 2014	Apporter des changements administratifs et fournir les réponses du Canada aux questions de l'industrie

ANNEXE A

ÉNONCÉ DES TRAVAUX

1. Objectif

Acquérir des services informatiques professionnels de six (6) catégories différentes fournis par le secteur privé en utilisant l'arrangement en matière d'approvisionnement des services professionnels en informatique centrés sur les tâches, selon les besoins.

2. Services partagés Canada – Contexte

Services partagés Canada (SPC) a été créé le 4 août 2011 dans le but de transformer radicalement la façon dont le gouvernement du Canada assure la gestion de son infrastructure de technologie de l'information (TI). Son mandat consiste à regrouper et à exploiter les services de centres de données, de réseaux et de messagerie électronique avec le concours d'organismes centraux et des partenaires de SPC. Le mandat relatif à la prestation des services d'infrastructure de TI pangouvernementaux est d'offrir le meilleur rapport qualité-prix ainsi qu'une infrastructure de TI plus fiable pour appuyer les opérations d'un gouvernement moderne.

3. Programme de transformation de la cybersécurité et de la sécurité de la TI – Contexte

Le mandat de Transformation de la cybersécurité et de la sécurité de la TI est le suivant : « Dans le cadre du mandat de SPC, la division Transformation de la cybersécurité et de la sécurité de la technologie de l'information est chargée de l'élaboration de plans et de la conception des services de cybersécurité et de sécurité des TI liés à l'infrastructure des TI du GC, jusqu'au niveau secret, dans les limites du mandat de SPC. Cette division élaborera des analyses de rentabilisation relatives aux services de l'infrastructure secrète et de la sécurité des TI prêts à être conçus. De plus, elle établira et améliorera de façon continue des solutions stratégiques de sélection des fournisseurs, des contrôles de sécurité et une architecture opérationnelle pour la mise en œuvre et la prestation de services transformés. Elle établit également des relations stratégiques avec des organismes centraux et les partenaires de SPC, afin d'élaborer des politiques, des normes, des directives technologiques et une surveillance continue pour la gestion et la prestation des services de cybersécurité et de sécurité des TI.

4. Portée des travaux

La division Transformation de la cybersécurité et de la sécurité de la technologie de l'information de Services partagés Canada a besoin, de manière ponctuelle, de faire appel à des professionnels des TI pour assurer la sécurité des TI et pour participer à l'élaboration du Programme de transformation de la cybersécurité et de la sécurité de la TI. La Division a besoin de services professionnels fournis par des prestataires expérimentés et réactifs, titulaires d'une attestation de sécurité de niveau Secret et possédant une parfaite maîtrise de différentes technologies en GI-TI. Les travaux confiés seront lancés au moyen d'un processus d'autorisation de tâches.

Les travaux exécutés en vertu du présent contrat fourniront un appui et des services en matière de sécurité des TI dans tous les domaines désignés, classifiés et non classifiés pour tous les programmes et

projets de transformation de SPC se rapportant aux sous-programmes de la Division, y compris les suivants :

4.1 Sous-programme relatif à la cybersécurité

- ***Portée :*** *développement et renforcement constant de la capacité de SPC à défendre le Canada contre les cybermenaces émergentes grâce à une meilleure connaissance de la situation et à l'évaluation du potentiel de risque et de l'incidence de l'élaboration de stratégies d'atténuation. Cela comprend l'élaboration de cyberstratégies, de normes, de lignes directrices, d'évaluations des menaces et d'études d'impact.*
- ***Fonctions :***
  - *Évaluer les cybermenaces et être au fait de la situation.*
  - *Veiller à l'intégrité de la chaîne d'approvisionnement.*
  - *Assurer la planification stratégique et élaborer des politiques en matière de cybersécurité.*

4.2 Sous-programme de services de sécurité des TI

- ***Portée :*** *regroupement et normalisation des services de sécurité des TI répertoriés ci-dessous pour les infrastructures non classifiées, désignées* et secrètes. Ce sous-programme fournit des services de planification continue, de surveillance et de conseils, ainsi que des directives relatives à la conception, la mise en œuvre et l'exploitation de ces services.*
- ***Fonctions :***
  - *Fournir des conseils et des directives en matière de sécurité des TI et élaborer des contrôles de sécurité pour les quatre programmes de transformation visés par le mandat de SPC (environnement informatique réparti, regroupement des centres de données, programme de transformation des télécommunications, appareils technologiques en milieu de travail), les initiatives de consolidation des applications des services administratifs du Secrétariat du Conseil du Trésor, les partenaires tripartites en matière de sécurité (Centre de la sécurité des télécommunications Canada, Secrétariat du Conseil du Trésor), les projets des partenaires et la Direction générale des opérations de SPC.*
  - *Élaborer des approches stratégiques et formuler des commentaires sur les plans stratégiques, afin de renforcer l'efficacité des stratégies de sécurité des TI, des stratégies de sélection des fournisseurs et des politiques en matière de TI.*
  - *Mettre en place des services de gestion de l'identité, des justificatifs d'identité et de l'accès.*
  - *Transformer les services de sécurité des réseaux au niveau du réseau.*
  - *Transformer les services de sécurité des appareils relativement aux appareils des utilisateurs finaux et des appareils dorsaux.*

4.3 Sous-programme relatif à l'infrastructure secrète du gouvernement du Canada (ISGC)

- ***Portée :*** *conception, élaboration et mise en œuvre de l'infrastructure secrète du gouvernement du Canada pour les services communs et essentiels, afin de satisfaire aux exigences de traitement de niveau Secret.*
- ***Fonctions :***
  - *Élaborer le programme d'infrastructure secrète du gouvernement du Canada.*
  - *Définir les projets du programme d'infrastructure secrète du gouvernement du Canada, les planifier et les coordonner.*

4.4 Définition des exigences en matière de sécurité au sein du Ministère et services d'intégration

- ***Portée :*** *définition des exigences en matière de sécurité afin d'assurer la prestation de services de sécurité stables à SPC dans le cadre des programmes de transformation, des projets de ses partenaires et d'autres initiatives gouvernementales définies.*
- ***Fonctions :***
  - *Ce service fournira les activités essentielles suivantes :*
  - *la définition de profils de sécurité;*
  - *la définition de contrôles de sécurité;*
  - *la fourniture de conseils et d'une orientation en matière de sécurité;*
  - *une liaison en matière d'exigences de sécurité avec le Centre de la sécurité des télécommunications Canada et le Secrétariat du Conseil du Trésor.*
  - *Ce service fournira l'activité de programme suivante afin d'appuyer les programmes de transformation et les projets des partenaires :*
  - *la définition des exigences en matière de sécurité à l'appui des documents d'approvisionnement (demandes de propositions, contrats, énoncés des travaux, etc.).*

5. Besoins en personnel

L'entrepreneur doit fournir des services professionnels en informatique dans six (6) catégories de ressources différentes, en fonction des besoins :

CATÉGORIE DE RESSOURCE	NIVEAU	Nº des SPICT
Analyste des activités en TI	Niveau III	B1
Spécialiste en protection et en planification de la sécurité des TI	Niveau III	C1
Spécialiste de la certification et de l'accréditation et des évaluations de la menace et des risques des TI	Niveau III	C3
Spécialiste de la conception de la sécurité des TI	Niveau III	C7
Spécialiste des analyses de vulnérabilité de la sécurité des TI	Niveau III	C11
Spécialiste de la protection des renseignements personnels	Niveau III	C16

Ces services professionnels sont requis dans un grand nombre de projets liés au mandat décrit ci-dessus ou dans le cadre d'activités générales de projets connexes, y compris : l'architecture d'entreprise, l'architecture de sécurité, les évaluations ou les certifications, ou encore la gestion de projet.

Le niveau d'effort et la durée des projets peut varier (de deux semaines à plus de deux ans). Le personnel de l'entrepreneur qui participe à des projets de courte ou de longue durée doit être prêt à exécuter les mêmes tâches répétitives. Le personnel de l'entrepreneur participant à des projets de longue durée peut être appelé à participer à l'ensemble du projet ou uniquement au volet du projet touchant son domaine d'expertise (sans doute au sein d'une équipe de projet déjà formée).

Les services requis seront associés à une ou à plusieurs des activités énumérées ci-dessous (remarque : la liste des activités répertoriées n'inclut pas l'intégralité des activités que pourrait devoir exécuter le personnel de l'entrepreneur).

5.1 Description des rôles

Voici une description des tâches et fonctions proposées que devra exécuter chaque catégorie de ressources.

5.1.1 Analyste des activités en TI – B1, niveau 3

Les responsabilités suivantes sont associées au présent énoncé des travaux (sans toutefois s'y limiter) :

1) Élaborer, examiner et gérer les exigences opérationnelles.
2) Planifier et coordonner des réunions avec les ministères et les organismes partenaires de SPC, en rendre compte et en assurer le suivi en vue de recueillir les exigences opérationnelles, d'établir la priorité de ces dernières et d'en déterminer l'incidence sur les activités, les modèles de coûts et les dépendances sur le plan opérationnel.
3) Effectuer une analyse des exigences opérationnelles afin de déterminer et d'étayer par écrit les rôles et les responsabilités de SPC et de ses partenaires.
4) Effectuer une analyse des exigences opérationnelles afin de déterminer et de consigner l'information, les procédures et les flux décisionnels, ainsi que les politiques connexes.
5) Rendre compte des cas d'utilisation actuels associés aux exigences opérationnelles.
6) Obtenir l'approbation officielle écrite des partenaires de SPC quant au document de spécification des exigences opérationnelles et gérer le processus afférant.
7) Établir des critères d'essais d'acceptation avec le client.
8) Appuyer et employer les méthodologies ministérielles sélectionnées.
9) Documenter les mesures et les décisions prises en réunion, les examiner avec les intervenants concernés et en assurer le suivi.
10) Déterminer et documenter les processus opérationnels actuels (activités ou opérations).
11) Fournir une orientation aux architectes techniques et aux développeurs, afin de répondre aux exigences fixées.
12) Préparer des exposés à l'intention des intervenants ou des cadres supérieurs.
13) Effectuer une analyse des exigences fonctionnelles afin d'en dégager les données, les procédures et les flux décisionnels.
14) Déterminer et évaluer les procédures, les méthodes et les éléments existants, comme le contenu et la structure des bases de données.
15) Définir et documenter les interfaces des opérations manuelles vers les opérations automatisées au sein des sous-systèmes d'application, vers des systèmes externes, et entre les systèmes, nouveaux et existants.
16) En collaboration avec divers intervenants et d'autres sources, comprendre et cibler tous les renseignements relatifs aux exigences se rapportant au projet. Faciliter la tenue de réunions et d'exercices interfonctionnels pour vérifier la situation actuelle, rendre compte des exigences et assurer l'harmonisation des projets de cybersécurité avec les initiatives et les programmes de transformation existants.
    - Planifier et mettre en œuvre toutes les activités relatives aux exigences, y compris leur obtention, leur validation, la présentation de rapport de situation, la résolution des conflits et l'obtention d'approbations.
17) Élaborer des exigences opérationnelles et fonctionnelles détaillées pour les projets relatifs à la cybersécurité et gérer le processus afférant, en préparant des cas d'utilisation et des modèles de données, et en rendant compte des règles

opérationnelles existantes provenant de diverses formes de documents, comme les schémas de processus et les entrevues avec des experts du domaine. Organiser, structurer et comprendre les exigences collectées, les rendre exploitables, effectuer les vérifications nécessaires et les valider.

- Gérer les exigences en elles-mêmes, et effectuer notamment un contrôle des changements apportés aux exigences et un contrôle de leur portée.

18) Participer à l'élaboration et à la conception détaillées en gérant les modèles de processus à venir, en effectuant des analyses des problèmes et en veillant à ce que les équipes techniques et d'architecture comprennent les objectifs opérationnels et les capacités fonctionnelles sous-jacents nécessaires à la réussite du projet.

Il s'agit de contribuer à l'élaboration et à la fourniture de deux systèmes de rappel sur l'infrastructure de cybersécurité, un provisoire et un plus durable, en travaillant en collaboration avec différents intervenants et experts du domaine pour recueillir, analyser, modéliser, communiquer et valider les exigences d'architecture et de conception.

Si l'échéancier le permet, l'analyste des activités peut être amené à effectuer d'autres travaux visant à appuyer le programme relatif à la cybersécurité.

Dans le cadre desdits travaux, il pourra être demandé à l'entrepreneur de fournir une aide en matière de gestion de projet pour l'une ou l'autre des tâches détaillées ci-dessous à d'autres professionnels dont les tâches relèvent du programme relatif à la cybersécurité.

Soutien général au programme :

a) Élaborer des documents d'affaires, comme des analyses de rentabilisation et des propositions d'investissement stratégique, et assurer l'harmonisation avec le plan d'activités de la direction.

b) Analyser et documenter les processus opérationnels nouveaux et existants afin d'appuyer les objectifs des projets et du programme relatif à la cybersécurité.

c) Aider les gestionnaires de projet à préparer des arrêtés de projet, des énoncés des travaux de même que des plans et des calendriers de projet. Aider les gestionnaires de projet à mener à bien les processus qui appuient les domaines de planification de la gestion de projet, tels que les processus de contrôle des changements, le suivi des problèmes, la gestion des risques et les processus d'établissement des bornes de SPC.

5.1.2 Spécialiste en protection et en planification de la sécurité des TI – C1, niveau 3

Les responsabilités suivantes sont associées au présent énoncé des travaux (sans toutefois s'y limiter) :

1) Examiner, analyser ou appliquer les politiques, les procédures et les lignes directrices en matière de sécurité des TI de gouvernements étrangers, du gouvernement fédéral ou d'un gouvernement provincial ou territorial.
2) Examiner, analyser et appliquer les meilleures pratiques de sécurité des TI, le droit national et international et de l'éthique en informatique, l'architecture de sécurité des TI et les méthodes de gestion des risques pour la sécurité des TI.
3) Élaborer des documents d'orientation décrivant les moyens d'assurer que la sécurité des TI et la cyberprotection soient des instruments opérationnels.

4) Effectuer des analyses des fonctions opérationnelles et des évaluations des impacts opérationnels.
5) Informer les cadres supérieurs.
6) Fournir des évaluations stratégiques des tendances technologiques et des nouvelles technologies.
7) Offrir des services de consultation et de planification stratégique sur la sécurité des TI.
8) Réaliser des études de faisabilité, des évaluations des technologies et des analyses de rentabilité, et proposer des plans de mise en œuvre des systèmes liés à la sécurité des TI.
9) Élaborer des politiques et des stratégies de R. et D. sophistiquées.
10) Recueillir, compiler et prioriser les besoins du client en matière de protection de l'infrastructure de l'information et de sécurité des TI.
11) Évaluer les outils technologiques dans l'ensemble de l'organisation et participer à leur sélection.
12) Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.
13) Élaborer une vision, des stratégies et des concepts stratégiques pour l'architecture de sécurité des TI à l'aide du Programme de facilitation de la transformation opérationnelle et du Modèle de référence stratégique du gouvernement du Canada (MRSG).
14) Élaborer des programmes et des concepts de service en matière de sécurité des TI à l'aide des MRSG suivants : le Modèle de la logique du programme, le Modèle d'harmonisation des programmes et services, le Modèle de responsabilisation et d'intégration des services, le Modèle de transition de l'état, le Modèle d'information et le Modèle de rendement.
15) Préparer et fournir du matériel de formation adapté à la catégorie de ressources.
16) Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.

5.1.3 Spécialiste de la certification et de l'accréditation et des évaluations de la menace et des risques des TI – C3, niveau 3

Les responsabilités suivantes sont associées au présent énoncé des travaux (sans toutefois s'y limiter) :

1) En s'appuyant sur la Méthodologie harmonisée d'évaluation des menaces et des risques du gouvernement du Canada, élaborer et documenter des énoncés de sensibilité, déterminer les agents de menace, les menaces et les scénarios de menace, effectuer des évaluations des menaces, déterminer les risques et les vulnérabilités potentiels, et recommander des mesures de protection et d'autres stratégies d'atténuation des risques pour l'infrastructure, les systèmes et les services pangouvernementaux en matière de TI indiqués par le responsable technique.
2) Élaborer et documenter l'ébauche et la version définitive d'un rapport d'évaluation des menaces.
3) Élaborer et documenter l'ébauche et la version définitive d'un rapport d'évaluation de la menace et des risques.
4) Rédiger un rapport faisant la synthèse des recommandations et des stratégies d'atténuation des risques destiné à la haute direction et à d'autres intervenants, documentation technique détaillée à l'appui.
5) Travailler en partenariat avec tous les intervenants afin de déterminer l'architecture technique, les défis, les risques et les recommandations de divers projets de SPC relatifs aux programmes et aux initiatives de transformation de SPC.
6) Collaborer avec tous les intervenants afin d'évaluer les données pertinentes transmises par les fournisseurs de services, les équipes chargées de la transformation, les équipes de gestion de projet et les équipes opérationnelles.
7) Réaliser les tâches nécessaires pour appuyer directement le programme de transformation de la cybersécurité et de la sécurité de la TI du gouvernement du Canada

et de SPC, ainsi que d'autres programmes de transformation en matière de cybersécurité et de sécurité des TI.

8) Élaborer différents dispositifs de sécurité, le cas échéant.
9) Participer à des réunions et des discussions relatives à la sécurité des TI et présenter des exposés aux intervenants ou à la haute direction.
10) Documenter, examiner et assurer le suivi des mesures et des décisions prises lors des réunions.
11) Effectuer une analyse fonctionnelle ou une analyse des options afin d'appuyer la réalisation du programme.
12) Mener une analyse d'impact en vue de concevoir une solution destinée au Ministère, l'évaluer et formuler des recommandations.
13) Préparer des exposés et les présenter à différents intervenants. Animer des réunions et des discussions.
14) Examiner les énoncés de sensibilité et les énoncés du niveau acceptable de risque.
15) Repérer les agents de menace, définir les scénarios de menace, déterminer les risques et les vulnérabilités potentiels, et formuler des recommandations concernant les mesures de protection et les autres stratégies d'atténuation des risques portant sur l'infrastructure des TI, des systèmes, des applications et des services désignés par le responsable technique, en prenant soin de réutiliser l'information autant que possible.
16) Vérifier que les mécanismes de sécurité des applications, des systèmes et des infrastructures respectent les politiques et les normes applicables.
17) Vérifier que les mécanismes de sécurité nécessaires ont bien été mis en œuvre.
18) Évaluer les risques résiduels mis au jour par l'évaluation des risques et vérifier que leur niveau est acceptable.
19) Examiner les résultats de l'évaluation de sécurité afin de veiller au bon fonctionnement du système et de garantir que les risques entourant son exploitation sont acceptables. Veiller à ce que le système respecte les politiques et les normes de sécurité ministérielles pertinentes.
20) Aider l'autorité de certification à évaluer les preuves de certification.
21) Produire un certain nombre de modèles de documents de la division Transformation de la cybersécurité et de la sécurité de la TI ou de la Direction de l'acquisition de systèmes informatiques et de télécommunications, tels que : des rapports d'autorisation et d'évaluation de la sécurité, des notes d'information, des profils de contrôle de sécurité fondés sur le document ITSG-33 et des évaluations des menaces et des risques, ainsi que d'autres types d'évaluations de sécurité.
22) Rédiger des rapports de certification et des lettres d'accréditation en fonction de l'état des mesures de protection choisies et mises en œuvre.
23) Observer la réalisation de tests de sécurité, s'il y a lieu.
24) Examiner les plans de mise en œuvre de mesures de protection et en faire la critique.
25) Vérifier les résultats des tests de sécurité, la validation de sécurité et le respect de la liste de vérification de la sécurité.
26) Collaborer dans le cadre de la recherche des exigences de sécurité, des attributs et des mesures de protection qui permettent d'améliorer le profil de sécurité du système.
27) Aider les partenaires commerciaux à élaborer des exigences relatives à la sécurité (énoncé de sensibilité, catégorisation des biens, modélisation des menaces, besoins opérationnels en matière de sécurité, énoncé du niveau acceptable de risque, etc.).
28) Évaluer les documents relatifs à l'architecture de référence et à l'architecture technique ainsi que les documents de conception détaillée, dans la mesure où ils s'appliquent à la sécurité.
29) Évaluer les contrôles de sécurité des TI (fondés sur le document ITSG-33) et les mesures de protection.
30) Évaluer les stratégies d'atténuation.
31) Évaluer le risque résiduel.
32) Au besoin, animer des séances de sensibilisation à la sécurité des TI.

33) Élaborer d'autres documents ou rapports techniques ponctuels, à la demande de l'autorité de certification.
34) L'examen des preuves de l'évaluation et de l'autorisation de sécurité comprend la préparation d'un rapport de certification de SPC et de la liste de preuves s'y rapportant. Les documents à examiner pour préparer le rapport et la liste incluent, sans toutefois s'y limiter, le questionnaire d'évaluation des facteurs relatifs à la vie privée, l'énoncé de sensibilité, les diagrammes d'architecture, l'énoncé du niveau acceptable de risque, le plan de tests et d'évaluation de sécurité, le rapport d'évaluation de la vulnérabilité, le plan de mise en œuvre de mesures de protection, le concept des opérations et la matrice de traçabilité des exigences relatives à la sécurité.
35) Concept des opérations de sécurité
36) Fournir un aperçu des besoins en matière de sécurité (du point de vue de la gestion de la protection des renseignements personnels, de l'organisation, de l'administration, de l'effectif, des techniques, des procédures et des mesures d'urgence) auxquels la solution de conception définitive du système est sensée répondre.
37) Fournir un aperçu contextuel des fonctions du projet en matière de sécurité (schémas logiques, circonstances, conditions et préoccupations opérationnelles particulières) que la conception de la sécurité du système doit permettre d'exécuter.
38) Conception de l'architecture
39) Décrit la définition du concept, la conception logique, la conception du réseau et la conception physique du point de vue de la sécurité.
40) Mener des évaluations de la menace et des risques comprenant :
41) un énoncé de sensibilité;
42) une évaluation des menaces;
43) une évaluation non technique de la vulnérabilité;
44) une évaluation des risques;
45) des recommandations pour l'atténuation des risques;
46) un questionnaire d'évaluation des facteurs relatifs à la vie privée;
47) une matrice de traçabilité des exigences en matière de sécurité;
48) un plan de tests et d'évaluation de sécurité;
49) un plan répertoriant les éléments à tester et à évaluer, une procédure décrivant la marche à suivre et les résultats des tests et de l'évaluation;
50) une évaluation de la vulnérabilité et des essais de pénétration.
51) Élaborer un plan d'évaluation de la vulnérabilité.
52) En consultation avec les parties concernées, réaliser des évaluations de la vulnérabilité et des essais de pénétration (ou les observer dans certains cas) et en documenter les résultats.
53) Plan de mise en œuvre de mesures de protection
54) Mettre en valeur les lacunes constatées pendant les activités officielles de test et d'évaluation de la sécurité ou dans la version définitive de l'évaluation de la menace et des risques. Formuler des recommandations pour remédier aux points portant atteinte à l'objectif de sécurité fixé.
55) Fournir la preuve que les services ou les applications et l'infrastructure respectent les exigences documentées dans les produits livrables susmentionnés, y compris :
56) la vérification de la conformité des mécanismes de sécurité aux politiques et aux normes applicables;
57) la validation des exigences de sécurité par la mise en correspondance de la politique de sécurité propre au système et des exigences de sécurité fonctionnelles et par le suivi des exigences de sécurité tout au long de l'élaboration des spécifications du système;
58) la vérification que les mesures de protection ont été mises en œuvre correctement et respectent les normes en vigueur. 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;
59) les tests et l'évaluation de sécurité afin de déterminer que les mesures de protection techniques fonctionnent correctement.

60) Examiner les produits livrables ci-dessous et fournir des commentaires écrits s'y rapportant :
    - plan de gestion de programme;
    - plan de gestion des renseignements personnels;
    - plan de continuité des services;
    - rapports d'évaluation des risques en matière de sécurité.
61) Plans, documents et éléments de preuve fournis par l'entrepreneur et attestant d'un système de gestion de la sécurité de l'information certifié ISO 27001 ou équivalent

5.1.4 Spécialiste de la conception de la sécurité des TI – C7, niveau 3

Dans le cadre du présent contrat et sans toutefois s'y limiter, les responsabilités sont les suivantes :

1) Travailler en partenariat avec tous les intervenants afin de déterminer l'architecture technique, les défis, les risques et les recommandations de divers projets de SPC relatifs aux programmes et aux initiatives de transformation de SPC.
2) Collaborer avec tous les intervenants afin d'évaluer les données pertinentes transmises par les fournisseurs de services, les équipes chargées de la transformation, les équipes de gestion de projet et les équipes opérationnelles.
3) Réaliser les tâches nécessaires pour appuyer directement le programme de transformation de la cybersécurité et de la sécurité de la TI du gouvernement du Canada et de SPC, ainsi que d'autres programmes de transformation en matière de cybersécurité et de sécurité des TI.
4) Effectuer une analyse des évaluations de la situation actuelle afin d'appuyer les programmes essentiels de transformation en matière de cybersécurité et de sécurité des TI.
5) Élaborer différents dispositifs de sécurité, le cas échéant.
6) Participer à des réunions et des discussions relatives à la sécurité des TI et présenter des exposés aux intervenants ou à la haute direction.
7) Documenter, examiner et assurer le suivi des mesures et des décisions prises lors des réunions.
8) Effectuer une analyse fonctionnelle ou une analyse des options afin d'appuyer la réalisation du programme.
9) Mener une analyse d'impact en vue de concevoir une solution destinée au Ministère, l'évaluer et formuler des recommandations.
10) Préparer des exposés et les présenter à différents intervenants. Animer des réunions et des discussions.
11) Donner des formations relatives à la sécurité et sensibiliser les employés à ce sujet.
12) Les exigences en matière de sécurité des TI appuyant les programmes essentiels de transformation en matière de cybersécurité et de sécurité de la TI comprennent, sans toutefois s'y limiter :
    a) examiner les exigences opérationnelles et des exigences en matière de sécurité de TI de différents programmes et initiatives de SPC;
    b) collaborer avec tous les intervenants en vue d'élaborer des profils de contrôle de sécurité fondés sur le document ITSG-33 du Centre de la sécurité des télécommunications Canada et sur d'autres normes en matière de sécurité, afin d'appuyer différents projets de SPC relatifs aux programmes et aux initiatives de transformation;
    c) valider les exigences en matière de sécurité des TI par la mise en correspondance des exigences opérationnelles ou des exigences de sécurité tout au long des étapes du PMSSI;

d) analyser et évaluer les besoins et les documents client;
e) planifier, formuler, coordonner et documenter des recommandations pour l'élaboration de solutions adaptées aux besoins client;
f) réaliser une analyse fonctionnelle ou d'une analyse des options en vue d'appuyer la réalisation du programme;

g) réaliser une analyse d'impact en vue de concevoir une solution destinée à l'organisation, la réalisation d'une évaluation et la formulation de recommandations.

13) Élaborer des stratégies, des cadres, des méthodes, des feuilles de route, des tableaux d'évaluation, des matrices RACI, des politiques et des instruments dans les domaines suivants, sans toutefois s'y limiter :
   a) gestion des risques en matière de sécurité, y compris les méthodes d'évaluation des risques;
   b) évaluation et autorisation de sécurité;
   c) gestion et gouvernance du programme relatif à la sécurité, y compris la conception ou l'examen organisationnel ou fonctionnel et la production de rapports de conformité à l'échelle du programme de services de la TI ou de la sécurité de l'information;
   d) examen et analyse de différents produits livrables des initiatives de transformation de SPC ou du Secrétariat du Conseil du Trésor; vérification du respect, de la conformité et de l'harmonisation des produits livrables avec les stratégies, les principes, les méthodologies, les cadres, les programmes, les politiques, les instruments (directives, normes, lignes directrices) et les procédures en matière de sécurité des TI du gouvernement du Canada (Secrétariat du Conseil du Trésor, Centre de la sécurité des télécommunications Canada, Sécurité publique Canada, SPC, etc.);
   e) élaboration de normes, de procédures et de lignes directrices en matière de sécurité des TI conformes aux exigences de la Politique de sécurité nationale du gouvernement du Canada et de la Politique sur la sécurité du gouvernement du Secrétariat du Conseil du Trésor et appuyant les normes opérationnelles (p. ex. gestion de la sécurité des technologies de l'information), les politiques de sécurité des ministères et organismes, et d'autres normes, procédures et lignes directrices pertinentes;
   f) élaboration de politiques en matière de sécurité des TI dans les domaines de la garantie de sécurité des TI, des cadres uniformisés de certification et d'accréditation pour les systèmes de TI, de protection de l'infrastructure de l'information, de l'évaluation des produits, de la protection des renseignements personnels, de la planification de la continuité des opérations, de la planification d'urgence et de la reprise après sinistre, et de la recherche et développement;
   g) gestion des services de sécurité des TI.

14) La gestion des risques liés à la sécurité des TI comprend, sans toutefois s'y limiter :
   a) l'examen et l'analyse de différents produits livrables des initiatives de transformation de SPC ou du Secrétariat du Conseil du Trésor, ainsi que la vérification du respect, de la conformité et de l'harmonisation des produits livrables avec les stratégies, les principes, les méthodologies, les cadres, les programmes, les politiques, les instruments (directives, normes, lignes directrices) et les procédures en matière de sécurité des TI du gouvernement du Canada (Secrétariat du Conseil du Trésor, Centre de la sécurité des télécommunications Canada, Sécurité publique Canada, SPC, etc.);
   b) la formulation de recommandations pour l'atténuation des risques en matière de sécurité des TI et d'autres produits livrables connexes, le cas échéant.

Les autres exigences relatives aux produits livrables du sous-programme relatif à la cybersécurité sont les suivantes, sans toutefois s'y limiter :

15) participer à l'élaboration de tous les documents nécessaires (par exemple, les rapports, les feuilles de route, les dossiers de présentation) relatifs à différentes évaluations de la

situation actuelle (p. ex. la sécurité des communications, le centre local de protection de l'information);

16) documenter les processus liés à la sécurité des initiatives de transformation;
17) élaborer des demandes de propositions afin de contribuer au processus d'approvisionnement en logiciels et en matériel de sécurité destinés à être utilisés par SPC – Centre des opérations de protection.

Les autres exigences relatives aux produits livrables du sous-programme de services de sécurité des TI sont les suivantes, sans toutefois s'y limiter :

18) contribuer à l'élaboration ou à la rédaction des documents suivants afin d'appuyer la stratégie de sécurité des appareils :
    a) plan de projet,
    b) arrêté de projet,
    c) analyse de rentabilisation,
    d) plan de communication,
    e) définition des services, plan ou stratégie de gestion du changement et stratégie de mise en œuvre,
    f) stratégie d'approvisionnement, notamment : demande de renseignements, demande de propositions, énoncé des travaux,
    g) information sur la journée de l'industrie (p. ex. questions et réponses concernant la sécurité des appareils, exposés),
    h) outils d'évaluation de la sécurité et d'autorisation de sécurité (énoncé de sensibilité, concept des opérations, évaluations des menaces);
19) établir et valider des profils de contrôle de sécurité conformes au document ITSG-33, à l'appui de divers projets administratifs de SPC relatifs à la transformation des services de sécurité du périmètre du réseau;
20) préparer des exposés et les présenter aux différents intervenants. À la demande du responsable technique, animer des réunions et des discussions et en rendre compte;
21) fournir et documenter différents profils de contrôle de sécurité, rapports, analyses de sécurité, organigrammes techniques de projet, calendriers et autres documents connexes, à la demande du responsable technique.

Les autres exigences relatives aux produits livrables du sous-programme de définition des exigences en matière de sécurité au sein du Ministère sont les suivantes, sans toutefois s'y limiter :

22) documenter la collecte d'exigences et les commentaires relatifs à la garantie de la sécurité dans le cadre des projets de télécommunications et de communications convergentes de grande ampleur, ainsi que d'autres programmes de transformation de SPC;
23) élaborer et documenter des définitions de services pour les projets de télécommunications et de communications convergentes de projets, ainsi que pour d'autres programmes de transformation de SPC;
24) en s'appuyant sur le processus du cycle de vie du processus de PMSSI (ITSG-33), déterminer et documenter les contrôles de sécurité connexes à l'aide des orientations du gouvernement du Canada, de la National Institute of Standards and Technology et d'autres parties afin de les incorporer aux documents d'architecture d'entreprise, aux demandes de propositions et aux énoncés des travaux, et en vue de mener à bien le processus d'évaluation et d'autorisation de sécurité. Des commentaires seront nécessaires à compter de la phase d'élaboration du concept, et ce jusqu'à l'étape d'installation;
25) rédiger des rapports d'évaluation des menaces et les documenter.

5.1.5 Spécialiste des analyses de vulnérabilité de la sécurité des TI – C11, niveau 3

Dans le cadre du présent contrat et sans toutefois s'y limiter, les responsabilités et la portée des travaux sont les suivantes :

1) revoir, analyser ou appliquer :
    - les outils d'analyse des agents de menace et les autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prévisionnelle, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie,
    - les détecteurs d'accès entrant et les perceurs de mots de passe,
    - les services consultatifs publics en matière de vulnérabilité des TI,
    - les analyseurs de réseau et outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap,
    - les protocoles réseau (HTTP, FTP, Telnet),
    - les protocoles de sécurité Internet, comme SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP,
    - la sécurité sans fil,
    - les systèmes de détection d'intrusion, les pare-feu et des vérificateurs de contenu,
    - les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus);
2) déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques;
3) mener des examens et des analyses des journaux de sécurité des systèmes sur site;
4) recueillir, compiler, analyser et diffuser de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents;
5) préparer ou tenir des réunions d'information sur les menaces, les vulnérabilités ou les risques liés à la sécurité des TI;
6) réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI;
7) préparer et fournir du matériel de formation adapté à la catégorie de ressources.

5.1.6 Spécialiste de la sécurité des TI (protection des renseignements personnels), C16, niveau 3

Dans le cadre du présent contrat et sans toutefois s'y limiter, les responsabilités et la portée des travaux sont les suivantes :

1) analyser les préoccupations relatives aux services de SPC, élaborer et fournir des listes de vérification relatives à la protection des renseignements personnels aux fins d'examen et d'approbation, mener des évaluations des facteurs relatifs à la vie privée visant les services fournis par SPC et élaborer différents documents à la demande du Commissariat à la protection de la vie privée du Canada.
2) Les travaux doivent être réalisés conformément aux normes, aux politiques et aux meilleures pratiques suivantes :
3) la *Loi sur la protection des renseignements personnels* et la législation provinciale qui s'y rapporte;
4) les attentes du Commissariat à la protection de la vie privée relatives à la mise en œuvre d'évaluations des facteurs relatifs à la vie privée;
5) la dernière Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (modèle d'évaluation des facteurs relatifs à la vie privée de base);
6) le code type sur la protection des renseignements personnels (CSA-fQ830).

7) Gestion des dossiers
8) La ressource doit avoir une connaissance approfondie des normes, des politiques et des lignes directrices du gouvernement du Canada.
9) La ressource doit être titulaire d'une certification dans le domaine de la protection des renseignements personnels, de préférence délivrée par un organisme de certification reconnu dans le secteur.
10) Son rôle consiste à analyser les préoccupations relatives à la protection des renseignements personnels se rapportant aux services fournis par SPC.
11) Elle est chargée d'élaborer et de fournir une liste de vérification relative à la protection des renseignements personnels aux fins d'examen et d'approbation.
12) Elle doit effectuer des évaluations des facteurs relatifs à la vie privée des services fournis par SPC et consulter le personnel du secteur de programme et la Direction de l'accès à l'information et de la protection des renseignements personnels.
13) Elle doit préparer et mettre à jour (le cas échéant), des exposés, des notes d'information et des réponses aux lettres du Commissariat à la protection de la vie privée concernant les évaluations des facteurs relatifs à la vie privée réalisées ou à réaliser.
14) Elle doit participer à l'élaboration des activités relatives aux évaluations des facteurs relatifs à la vie privée et les examiner, conformément à la nouvelle Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor et aux politiques et instruments s'y rapportant (normes, processus, lignes directrices et procédures).
15) Elle doit évaluer les risques d'entrave à la vie privée et proposer des mécanismes ou des stratégies d'atténuation.
16) Elle doit examiner la documentation des projets, lorsqu'ils sont disponibles ou s'il y a lieu, y compris les démonstrations, les diagrammes de flux de données et les supports d'exposés.
17) Elle doit entamer des discussions sur les questions de protection des renseignements personnels et y participer.
18) Elle doit se réunir avec les membres du Commissariat à la protection de la vie privée du Canada afin de discuter des éléments des évaluations des facteurs relatifs à la vie privée et elle doit élaborer un compte rendu des décisions prises lors de chaque réunion. Elle doit effectuer le suivi de toutes les mesures à prendre définies.
19) Elle doit accuser réception des questions des intervenants ministériels avant d'élaborer la version finale du rapport sur l'évaluation des facteurs relatifs à la vie privée, examiner ces questions, puis fournir une réponse.
20) Elle doit assurer le suivi d'autres exigences en matière d'information et aborder les questions relatives à la protection des renseignements personnels et aux risques des politiques qui peuvent être décelés durant la phase d'analyse.
21) Elle doit examiner la documentation des projets relative aux problèmes informatiques, aux technologies et à l'architecture qui influencent les risques inhérents à la protection des renseignements personnels.
22) Elle doit produire des rapports relatifs au respect des politiques et des instruments connexes (p. ex. les directives, les normes, les processus, les lignes directrices et les procédures).
23) Elle doit produire la version définitive des rapports d'évaluation des facteurs relatifs à la vie privée dans un délai suffisant pour permettre l'examen des conclusions par tous les intervenants, y compris la Direction de l'accès à l'information et de la protection des renseignements personnels.
24) Elle doit achever les évaluations des facteurs relatifs à la vie privée et les notes d'information.

6.0 Produits livrables

- Les exigences réelles en ressources seront établies de manière ponctuelle au moyen d'une autorisation de tâches.
- En plus des services décrits dans chacune des catégories de ressources, il est attendu que toutes les ressources, parallèlement à l'exécution de leurs tâches, fournissent à un représentant d'une entité du GC des conseils techniques et transfèrent les connaissances fonctionnelles par l'intermédiaire de documents écrits et de formations individuelles ou en groupe.
- L'entrepreneur doit fournir les produits livrables au responsable technique ou à son représentant (l'ébauche, la version finale ou les deux), tel qu'il est précisé dans chacune des autorisations de tâches. La portée et le contenu précis de chacun des produits livrables seront soumis au responsable technique pour qu'il les examine et en détermine l'acceptation.
- Les copies finales des produits livrables doivent contenir les commentaires reçus et les changements demandés par le responsable technique ou son représentant, et être livrées à la date d'échéance précisée dans chacune des autorisations de tâches ou avant cette date.
- Chaque ressource doit soumettre au responsable technique un rapport de situation hebdomadaire conforme au format de présentation précisé dans chacune des autorisations de tâches.
- Le calendrier, le format et le contenu de chaque produit livrable doivent être précisés dans l'autorisation de tâches, et l'entrepreneur doit y consentir par écrit. Ils doivent être conformes aux normes organisationnelles des autorisations de tâches (p. ex. utilisation d'un modèle d'exigences opérationnelles, d'une architecture normalisée pour les consultations opérationnelles, etc.).
- Les documents qui constituent des produits livrables doivent être remis en formats papier et électronique et avoir été créés à l'aide de la suite logicielle Microsoft Office. L'entrepreneur et le responsable technique pourront également convenir d'un autre format, le cas échéant.
- Rapport d'étape (de situation) L'entrepreneur est tenu de rédiger un rapport d'étape et de situation concernant le travail effectué dans le cadre du projet. Ledit rapport doit être joint à la feuille de temps mensuelle. Le rapport d'étape devra contenir au minimum les renseignements suivants :
    - toutes les activités importantes exécutées par l'entrepreneur pendant cette période;
    - l'état de toutes les mesures et décisions, ainsi qu'une liste des activités en cours;
    - une description des problèmes survenus qui sont susceptibles d'exiger l'attention du responsable technique, ainsi que toute recommandation utile à l'exécution des travaux;
    - la liste des jalons et leur date prévue, les progrès réalisés depuis le dernier rapport, les problèmes survenus et les prochaines étapes;
    - les heures consacrées par l'entrepreneur à la tâche durant la période du rapport;
    - les attentes et les produits livrables du mois, de la semaine ou du trimestre suivant.
- Le rapport d'étape et la feuille de temps doivent être transmis avec la facture.
    - L'appendice D de l'annexe B – Rapport de situation mensuel

7. Format des produits livrables

Les rapports d'étape doivent être transmis au responsable technique par courriel.

Les documents non classifiés et Protégé A peuvent être envoyés par courriel à l'aide du système de courriel du gouvernement du Canada. Les documents Protégé B doivent être chiffrés à l'aide d'une clé ICP du gouvernement du Canada, puis être transmis à l'aide du système de courriel du gouvernement du Canada. Les documents classés Secret (le cas échéant) doivent comprendre une copie papier et un exemplaire électronique (CD, DVD ou clé USB), et doivent être remis en mains propres au responsable technique.

Les produits livrables doivent pouvoir être modifiés à l'aide de la suite Microsoft Office (p. ex. Word, Excel, PowerPoint et Visio) version 2007 ou ultérieure.

8. Réunions courantes

Le chargé de projet de l'entrepreneur est tenu de se réunir avec le responsable technique ou son représentant, selon les priorités ou sur demande pour discuter de tout problème relatif à la prestation des services professionnels en informatique demandés. Ces rencontres sont sans frais supplémentaires.

9. Niveaux de service

9.1 Heures normales de travail

Les heures normales de travail sont de 7 h à 18 h (HE), du lundi au vendredi (à l'exception des jours fériés de la province où les travaux sont exécutés). L'entrepreneur doit travailler 7,5 heures par jour pendant les heures normales de travail, sauf si d'autres ententes sont prévues avec le responsable technique. Ce dernier autorisera des heures supplémentaires à l'avance, au même tarif que celui s'appliquant aux heures normales de travail. En règle générale, l'entrepreneur travaillera sur le site pendant les heures régulières de travail, à moins d'avoir conclu un accord au préalable avec le responsable technique. Pendant la durée du contrat, tous les membres du personnel doivent être prêts à travailler en dehors des heures normales de bureau, au besoin.

9.2 Lieu de travail

Les travaux de l'entrepreneur seront réalisés dans les locaux de Services partagés Canada ou hors site (à la discrétion du responsable ou du gestionnaire technique). Services partagés Canada est situé dans la région de la capitale nationale, et l'accès aux systèmes et à l'infrastructure de TI sera accordé, au besoin. Pendant la durée du contrat, le principal lieu de travail de Services partagés Canada ou de ses directions générales est susceptible de changer, mais demeurera dans la région de la capitale nationale. Services partagés Canada ne remboursera pas à l'entrepreneur les coûts associés à cette transition. L'entrepreneur est tenu d'assister aux réunions organisées par Services partagés Canada et les principaux intervenants du gouvernement du Canada, mais aucun déplacement important ne sera nécessaire. Tous les frais de déplacement dans la région de la capitale nationale sont assumés par l'entrepreneur.

À la demande d'un responsable technique, il est possible que certains travaux doivent être réalisés hors site, dans une infrastructure fournie par l'entrepreneur.

9.3 Exigences relatives aux déplacements

Aucun déplacement n'est nécessaire dans le cadre du présent énoncé des travaux. Cependant, si des déplacements sont nécessaires, les frais de déplacement et de subsistance s'appliqueront seulement si l'entrepreneur est tenu de travailler à l'extérieur de la région de la capitale nationale. S'il y a lieu, le chargé de projet doit autoriser les déplacements par écrit et à l'avance.

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. Le prix des billets d'avion ne doit pas être supérieur à celui de la classe économique.

9.4 Rapports hiérarchiques

Sur le plan fonctionnel, la ressource relèvera du responsable ou du gestionnaire technique.

10. Exigences relatives à la sécurité

La ressource doit disposer d'une attestation de sécurité de niveau Secret au minimum tout au long de la durée du contrat. Le soumissionnaire doit préciser le numéro de dossier de l'attestation de sécurité et sa date d'échéance.

11. Non-divulgation

Tous les travaux exécutés par l'entrepreneur dans le cadre du présent énoncé des travaux demeureront la propriété de l'État. Les rapports, documents et prolongations afférentes demeurent la propriété de l'État, et l'entrepreneur ne pourra divulguer ou diffuser de tels rapports ou documents à une autre personne, ni les reproduire, sans l'autorisation écrite préalable de l'État.

12. Renseignements exclusifs

Tous les renseignements et les documents mis à la disposition de l'entrepreneur dans le cadre du présent projet sont jugés exclusifs et devront être restitués à l'État une fois les tâches décrites dans le présent énoncé des travaux réalisées ou à la résiliation du contrat.

13. Interprétation

En cas de différends dans l'interprétation du présent énoncé des travaux ou de la terminologie qu'il contient, la décision du responsable technique aura préséance.

PIÈCE JOINTE 2 DE LA PARTIE 4

ÉVALUATION FINANCIÈRE DE LA PROPOSITION

(TABLEAU DES PRIX)

Le soumissionnaire devrait remplir ce barème de prix, puis le joindre à sa soumission financière.

Au minimum, le soumissionnaire doit répondre à ce barème de prix dans sa soumission financière en y incluant, pour chacune des périodes précisées ci-dessous, le tarif journalier ferme tout compris (en dollars canadiens) proposé pour chacune des catégories de personnel indiquées

PÉRIODE INITIALE DU CONTRAT (1 AN)	
Catégorie de personnel	**Taux journalier ferme proposé par le soumissionnaire**
Systèmes de gestion des activités	
Analyste de entreprise – Niveau 3	
Services de cyberprotection	
Spécialiste en protection et en planification de la sécurité des TI – Niveau 3	
Spécialiste de l'évaluation de la menace et des risques et de la certification et de l'accréditation – Niveau 3	
Spécialiste de la conception de la sécurité des TI – Niveau 3	
Spécialiste des analyses de vulnérabilité de la sécurité des TI – Niveau 3	
Spécialiste de la protection des renseignements personnels – Niveau 3	

PREMIÈRE ANNÉE D'OPTION (1 AN)	
Catégorie de personnel	**Taux journalier ferme proposé par le soumissionnaire**
Systèmes de gestion des activités	
Analyste de entreprise – Niveau 3	
Services de cyberprotection	
Spécialiste en protection et en planification de la sécurité des TI – Niveau 3	

Spécialiste de l'évaluation de la menace et des risques et de la certification et de l'accréditation – Niveau 3	
Spécialiste de la conception de la sécurité des TI – Niveau 3	
Spécialiste des analyses de vulnérabilité de la sécurité des TI – Niveau 3	
Spécialiste de la protection des renseignements personnels – Niveau 3	

DEUXIÈME ANNÉE D'OPTION (1 AN)	
Catégorie de personnel	**Taux journalier ferme proposé par le soumissionnaire**
Systèmes de gestion des activités	
Analyste de entreprise – Niveau 3	
Services de cyberprotection	
Spécialiste en protection et en planification de la sécurité des TI – Niveau 3	
Spécialiste de l'évaluation de la menace et des risques et de la certification et de l'accréditation – Niveau 3	
Spécialiste de la conception de la sécurité des TI – Niveau 3	
Spécialiste des analyses de vulnérabilité de la sécurité des TI – Niveau 3	
Spécialiste de la protection des renseignements personnels – Niveau 3	

Taxes

a) Dans le présent contrat, tous les prix et toutes les sommes excluent la taxe de vente harmonisée (TVH), sauf indication contraire. La TVH vient s'ajouter au prix indiqué dans le présent contrat et est acquittée par le Canada.

APPENDICE A DE LA PIÈCE JOINTE 1 DE LA PARTIE 4

TABLEAU DE RÉPONSE : JOURS FACTURABLES POUR LA DEMANDE DE PROPOSITIONS

Nom du soumissionnaire : _____

Période de facturation (60 mois consécutifs) du _/___/___ au ___/___/___
(jj/mm/aa) (jj/mm/aa)

En fournissant une réponse, le soumissionnaire certifie que les jours facturables pris en compte font partie de la période de facturation indiquée ci-dessus pour toutes les catégories de ressource énumérées.

CATÉGORIE DE RESSOURCES	NOMBRE DE JOURS FACTURABLES					
	Renvoi au nº de référence de contrat _____	Renvoi au nº de référence de contrat _____	Renvoi au nº de référence de contrat _____	Renvoi au nº de référence de contrat _____	Renvoi au nº de référence de contrat _____	Total