



RETURN RESPONSES TO:

**RETOURNER LES
RÉPONSES À:**

C/O Mark Hall
Bid Receiving Shared Services
Canada | Services partagés Canada
700 Montreal Road
Ottawa, Ontario
K1A 0P7

**REQUEST FOR RESPONSES FOR
EVALUATION**

**DEMANDE DE RÉPONSES POUR
L'ÉVALUATION**

Comments - Commentaires

This document contains a Security
Requirement

Vendor/Firm Name and address

**Raison sociale et adresse du
fournisseur/de l'entrepreneur**

Issuing Office – Bureau de distribution

Shared Services Canada / Services partagés Canada
Procurement And Vendor Relationships
11 rue Laurier
Gatineau, Quebec
K1A 0S5

Title – Sujet Internet Interconnection Services - les Services d'interconnexion Internet	
Solicitation No. – N° de l'invitation 10026415/A	Date
Client Reference No. – N° référence du client : 12-0737	
GETS Reference No. – N° de reference de SEAG	
File No. – N° de dossier C71.10026415/A.EF	CCC No. / N° CCC - FMS No. / N° VME
Solicitation Closes – L'invitation prend fin at – à 02 :00 PM on – le May 17, 2013	Time Zone / Fuseau horaire Eastern Standard Time (EST) / Heure normale de l'Est (HNE)
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Inquiries to : - Adresser toutes questions à: Mark Hall	Buyer Id – Id de l'acheteur C71
Telephone No. – N° de téléphone : 819-956-0251	Email - Courriel mark.hall@ssc-spc.gc.ca
Destination – of Goods, Services, and Construction: Destination – des biens, services et construction : See Herein Voir aux présentes	
Delivery required - Livraison exigée See Herein / Voir aux présentes	Delivery Offered – Livraison proposée



SERVICES PARTAGÉS CANADA

Services d'interconnexion Internet

DEMANDE DE RÉPONSES POUR L'ÉVALUATION

DRPE no. : 10026415/A



DEMANDE DE RÉPONSES POUR L'ÉVALUATION SERVICES D'INTERCONNEXION INTERNET (SII) POUR SERVICES PARTAGÉS CANADA (SPC)

TABLE DES MATIÈRES

PART 1	RENSEIGNEMENTS GÉNÉRAUX ET INSTRUCTIONS À L'INTENTION DES RÉPONDANTS	4
1.1	Introduction	4
1.2	Parties de la DRPE	4
1.3	Aperçu du besoin en SII	5
1.4	Instructions, clauses et conditions uniformisées applicables à la DRPE	5
1.5	Présentation d'une réponse	6
1.6	Demandes de renseignements pendant la période de la DRPE	6
1.7	Amélioration du besoin au cours de l'étape de la DRPE	7
1.8	Lois applicables	7
PART 2	Instructions pour la préparation de la réponse	9
2.1	Instructions pour la préparation de la réponse	9
2.2	Contenu de la réponse	9
2.3	Exigences relatives à la sécurité	10
2.4	Établissement des prix	10
PART 3	APERÇU DU PROCESSUS D'APPROVISIONNEMENT	11
3.1	Aperçu	11
PART 4	PROCÉDURES D'ÉVALUATION ET SÉLECTION DES RÉPONDANTS QUALIFIÉS	12
4.1	Procédures d'évaluation	12
4.2	Critères techniques obligatoires	12
4.3	Étape 2 : Sélection de répondants qualifiés	12
PART 5	ATTESTATIONS	13
5.1	Programme de contrats fédéraux – Attestation	13
5.2	Attestation pour ancien fonctionnaire	14

ANNEXES À LA DRPE :

Annexe A : Formulaire de présentation de la réponse à la DRPE des SII

Annexe B : Liste de vérification des exigences relatives à la sécurité (LVERS)

Annexe C : Liste des produits de technologie de l'information (TI)

Annexe D : Version provisoire de la demande de propositions (DP)



DEMANDE DE RÉPONSES POUR L'ÉVALUATION SERVICES D'INTERCONNEXION INTERNET (SII) POUR SERVICES PARTAGÉS CANADA (SPC)

PART 1 RENSEIGNEMENTS GÉNÉRAUX ET INSTRUCTIONS À L'INTENTION DES RÉPONDANTS

1.1 Introduction

- 1.1.1 La présente demande de réponses pour l'évaluation (DRPE) est lancée par Services partagés Canada.
- 1.1.2 La présente DRPE vise à déterminer et sélectionner les répondants qualifiés pour les étapes suivantes du présent processus d'approvisionnement.
- 1.1.3 Un aperçu de l'ensemble du processus d'approvisionnement figure à la partie 3, Aperçu du processus d'approvisionnement.
- 1.1.4 Le Canada souhaite résoudre, dès le début, les problèmes liés à la fonctionnalité de sécurité grâce aux solutions commerciales proposées pour répondre au besoin en services d'interconnexion Internet (SII). Par conséquent, dans le cadre de la présente demande de réponses pour l'évaluation, le Canada approuvera au préalable la liste des produits de technologie de l'information qui est proposée comme partie de l'infrastructure de réseau ou du réseau de base qui sera connecté au réseau du Canada. Ce processus permettra d'éliminer les solutions qui constituent pour le Canada une vulnérabilité ou une menace envers la fonctionnalité. Il s'agit ici d'une question de sécurité dont la nature évolue au fil du temps. Toutefois, l'évaluation des solutions proposées sera appliquée de façon uniforme selon les menaces perçues au moment de la clôture de la DRPE.

1.2 Parties de la DRPE

Partie 1 Renseignements généraux et instructions à l'intention des fournisseurs : fournit un aperçu des exigences relatives aux SII, ainsi que des instructions, des clauses et des conditions applicables à la DRPE.

Partie 2 Instructions relatives à la préparation de la réponse : présente aux répondants les instructions visant la préparation de leur réponse à la DRPE.

Partie 3 Aperçu du processus d'approvisionnement : donne aux répondants un aperçu des étapes du processus d'approvisionnement.

Partie 4 Procédures d'évaluation et sélection des répondants qualifiés : décrit le déroulement de l'évaluation des réponses à la DRPE, les critères d'évaluation et la méthode de sélection des répondants qui continueront à participer au processus d'approvisionnement en SII après l'étape de qualification.

Partie 5 Attestations : comprend les attestations à fournir dans le cadre de la réponse à la DRPE.

Les annexes suivantes font partie de la présente DRPE :

Annexe A : Formulaire de présentation de la réponse à la DRPE des SII;

Annexe B : Liste de vérification des exigences relatives à la sécurité (LVERS);



Annexe C : Liste des produits de technologie de l'information (TI);
Annexe D : Version provisoire de la demande de propositions (DP)

La présente DRPE n'est pas une demande de propositions, une demande de soumissions ou un appel d'offres. Elle vise uniquement à présélectionner des répondants. Aucun marché ne sera attribué à la suite de la DRPE. Comme le Canada peut annuler la DRPE, les processus d'approvisionnement subséquents décrits dans le présent document peuvent ne pas voir le jour. Étant donné que la DRPE n'est pas un appel d'offres, les répondants peuvent se retirer du processus n'importe quand.

Les clauses du contrat subséquent, y compris l'énoncé des travaux, qui décrit le type de marché qui peut découler de la demande de propositions subséquente, ont été incluses dans le but d'aider les répondants dans l'élaboration de leur réponse.

1.3 Aperçu du besoin en SII

Le gouvernement du Canada (ci-après appelé le « Canada » ou le GC) a besoin d'un service d'interconnexion Internet (SII) en diversité qui lui permettra d'accéder aux services Internet publics, tout en contribuant à la prestation des programmes et services offerts aux Canadiens.

Le besoin en SII vise les services suivants, qui seront prêtés au fur et à mesure des besoins :

- services d'interconnexion Internet (SII);
- service de protection contre les attaques par déni de service distribué (DSD);
- déplacement de circuits;
- tout produit livrable exigé aux termes du marché.

Les services seront prêtés dans la région de la capitale nationale (RCN) et dans la région de Toronto (Toronto), au Canada, à l'exception des lieux soumis aux ententes sur la revendication territoriale globale. Le besoin comprend trois points d'interface de service (PIS) à redondance pour le SII fournis dans le cadre de deux ou trois contrats subséquents distincts, soit deux PIS dans la RCN et un PIS dans la région de Toronto. Chaque PIS doit offrir la capacité et la fiabilité nécessaires pour traiter le trafic Internet en cas de panne des autres. Le marché exigera la fourniture, au fur et à mesure des besoins, de PIS supplémentaires pour le SII à l'intérieur du même centre de données du GC ou d'autres centres de données du GC dans la RCN et la région de Toronto.

SPC se servira des marchés subséquents pour fournir des services partagés à ses clients, soit lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant le marché, et les autres organisations qui choisissent de recourir à ses services de temps en temps, à tout moment pendant le marché. L'objectif est d'attribuer deux ou trois marchés de trois ans chacun et comprenant une option irrévocable d'un an permettant au Canada de prolonger la durée du marché.

1.4 Instructions, clauses et conditions uniformisées applicables à la DRPE

- 1.4.1 Toutes les instructions, clauses et conditions de la demande de la DRPE sont identifiées par un numéro, une date et un titre dans le Guide des clauses et conditions uniformisées d'achat (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>), produit par Travaux publics et Services gouvernementaux Canada (TPSGC).
- 1.4.2 Toutes les mentions de TPSGC contenues dans les instructions uniformisées seront interprétées comme faisant référence à SPC.
- 1.4.3 Les répondants qui présentent une réponse s'engagent à respecter les instructions, les clauses et les conditions de la DRPE.



- 1.4.4 Le document 2003 (2012-11-19), Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la DRPE et en fait partie intégrante, sauf :
- 1.4.4.1 lorsque l'expression « demande de soumissions » est utilisée, la remplacer par « demande de réponses pour l'évaluation »;
 - 1.4.4.2 lorsque le terme « soumission » est utilisé, le remplacer par « réponse »;
 - 1.4.4.3 lorsque le terme « soumissionnaire » est utilisé, le remplacer par « répondant »;
 - 1.4.4.4 lorsque le terme « fournisseur » est utilisé, le remplacer par « répondant ».
 - 1.4.4.5 La présente DRPE ne concerne que la possibilité de se qualifier afin de présenter une soumission en réponse à une demande de propositions éventuelle pour les SII.
 - 1.4.4.6 Le paragraphe 5 (4), qui traite d'un délai de validité, ne s'applique pas étant donné que la DRPE invite seulement les fournisseurs à se qualifier. À moins que le répondant informe l'autorité contractante de son désir de retirer sa réponse, le Canada supposera qu'il tient toujours à se qualifier.
- 1.4.5 En cas de divergence entre les dispositions du document 2003 et ce document, ce dernier l'emporte. Toutes les mentions de TPSGC contenues dans les instructions uniformisées seront interprétées comme faisant référence à SPC.
- 1.4.6 Le texte du paragraphe 4 de la section 01 – Code de conduite et attestations, du document 2003 susmentionné est remplacé par ce qui suit :
- Les répondants doivent fournir avec leur réponse, ou le plus tôt possible après l'avoir déposée, une liste complète des personnes qui occupent actuellement un poste d'administrateur au sein de leur entreprise. Si la liste n'a pas été fournie à la fin de l'évaluation des réponses, le Canada informera le soumissionnaire du délai dans lequel l'information doit être fournie. Si cette liste n'est pas fournie dans le délai prescrit, la réponse sera déclarée irrecevable.
- Le Canada peut, en tout temps, demander aux répondants de fournir dans un délai donné un formulaire de consentement dûment rempli et signé ([Consentement à la vérification de l'existence d'un casier judiciaire – PWGSC-TPSGC 229](#)) pour les personnes inscrites sur la liste susmentionnée. Si le soumissionnaire ne fournit pas le formulaire de consentement dans le délai prescrit, sa réponse sera déclarée irrecevable.
- Le texte du paragraphe 5 de la section 01 – Code de conduite et attestations, du document 2003 susmentionné est remplacé par ce qui suit :
- Le répondant doit diligemment tenir à jour la liste en informant le Canada, par écrit, de tout changement survenant au cours de la période de validité de la réponse. Il doit également fournir au Canada les formulaires de consentement correspondants, au besoin. En outre, le répondant devra diligemment tenir à jour la liste et fournir, au besoin, les formulaires de consentement au cours de la période d'exécution de tout marché découlant de la présente invitation à soumissionner.

1.5 Présentation d'une réponse

- 1.5.1 Les réponses doivent être présentées uniquement au Module de réception des soumissions de SPC au plus tard à la date, à l'heure et à l'endroit indiqués sur la page couverture de la DRPE, en dépit des instructions du document 2003.
- 1.5.2 En raison du caractère de la DRPE, les réponses transmises par télécopieur à l'intention de SPC ne seront pas acceptées.

1.6 Demandes de renseignements pendant la période de la DRPE

- 1.6.1 Toutes les demandes de renseignements concernant la DRPE et la version provisoire de la DP doivent être présentées par écrit à l'autorité contractante au moins dix (10) jours civils avant la



date de clôture de la DRPE. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

- 1.6.2 Les répondants devraient indiquer le plus exactement possible le numéro d'article de la DRPE auquel renvoie leur demande de renseignements. Les répondants devraient prendre soin d'expliquer chaque question en donnant suffisamment de détails pour permettre au Canada d'y apporter des réponses exactes.
- 1.6.3 Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada pourra demander au répondant de modifier la question afin d'en éliminer le caractère exclusif, et y répondra en transmettant des copies des réponses à tous les répondants. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les répondants.
- 1.6.4 Le Canada a l'intention de répondre à toutes les questions concernant la version provisoire de la demande de propositions (DP) jointe en annexe à la DRPE, à l'étape de la DRPE. Afin de s'assurer que les répondants connaissent le besoin avant de répondre à la présente DRPE, l'autorité contractante ne répondra à aucune question au sujet de l'énoncé des travaux (ET) pendant l'étape de la DP. Les répondants devraient poser toutes les questions concernant l'ET du Canada décrit dans la version provisoire de la DP au cours de l'étape de la DRPE.

1.7 Amélioration du besoin au cours de l'étape de la DRPE

S'ils croient que les spécifications ou l'énoncé des travaux contenus dans la version provisoire de la demande de propositions (DP) pourraient être améliorés sur les plans technique ou technologique, les répondants sont invités à formuler des propositions, par écrit, à l'autorité contractante dont le nom est indiqué dans la version provisoire des clauses du contrat subséquent. Les répondants doivent décrire clairement les améliorations proposées et les motifs qui les justifient. Les propositions qui ne restreignent pas la concurrence ou qui ne favorisent pas un répondant en particulier seront examinées à la condition qu'elles soient présentées à l'autorité contractante conformément au paragraphe intitulé « Demandes de renseignements en période de réponse à la DRPE ». Le Canada aura le droit d'accepter ou de rejeter n'importe quelle ou la totalité des suggestions proposées.

1.8 Lois applicables

- 1.8.1 Les relations entre les parties seront régies par les lois en vigueur dans la province de l'Ontario.
- 1.8.2 À sa discrétion, un répondant peut indiquer les lois applicables d'une province ou d'un territoire canadien de son choix, sans que la validité de sa réponse soit remise en question, en insérant le nom de la province ou du territoire canadien de son choix dans le formulaire de présentation de la réponse à la DRPE qui se trouve à l'annexe A. Si aucune province ou territoire n'est précisé, le répondant reconnaît qu'il accepte les lois en vigueur dans la province de l'Ontario.

1.9 Présentation d'une seule soumission par un groupe soumissionnaire :

- 1.9.1.1 Il est interdit aux membres d'un même groupe de répondants de présenter plusieurs réponses à la présente DRPE. S'ils le font, le Canada les annulera toutes.
- 1.9.1.2 Aux fins du présent article, « **groupe de répondants** » s'entend des entités (qu'elles soient notamment formées d'une ou de plusieurs personnes physiques, de sociétés, de partenariats ou de sociétés de personnes à responsabilité limitée) liées entre elles. Peu importe la province ou le territoire ou elles ont été constituées en société ou formées juridiquement, on considère que les entités sont « **liées** » dans le cadre de la présente demande de soumissions si :



- 1.9.1.2.1 il s'agit de la même personne morale (c'est-à-dire la même personne physique, société, société de personnes à responsabilité limitée, le même partenariat, etc.);
- 1.9.1.2.2 il s'agit de « personnes liées » ou de « personnes affiliées » selon la *Loi de l'impôt sur le revenu du Canada*;
- 1.9.1.2.3 les entités entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire), ou en ont entretenu une au cours des deux dernières années ayant précédé la clôture des soumissions;
- 1.9.1.2.4 les entités n'ont aucun lien de dépendance entre elles ni avec le même tiers.



PART 2 INSTRUCTIONS POUR LA PRÉPARATION DE LA RÉPONSE

2.1 Instructions pour la préparation de la réponse

2.1.1 **Copies de la réponse** : Le Canada demande aux répondants de présenter leur réponse conformément aux exigences suivantes :

- 2.1.1.1 annexe A : formulaire de présentation de la réponse à la DRPE (1 copie papier);
- 2.1.1.2 annexe C : liste des produits de TI (1 copier papier) et 1 copie électronique sur CD ou DVD.
- 2.1.1.3 En cas de différence entre le libellé de la copie électronique et celui de la copie papier, ce dernier prévaut.

2.1.2 **Politique d'achats écologiques du Canada** : En avril 2006, le Canada a approuvé une politique exigeant que les organismes et ministères fédéraux prennent les mesures nécessaires pour incorporer les facteurs environnementaux dans le processus d'approvisionnement. Veuillez consulter la Politique d'achats écologiques (<http://tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html>). Pour aider le Canada à atteindre ses objectifs, on invite les répondants à :

- 2.1.2.1 utiliser du papier contenant des fibres certifiées provenant d'un aménagement forestier durable et/ou contenant au moins 30 % de matières recyclées;
- 2.1.2.2 utiliser un format qui respecte l'environnement : impression noir et blanc plutôt que couleur, impression recto verso, et des agrafes ou des trombones plutôt qu'une reliure Cerlox, une reliure à attaches ou une reliure à anneaux.

2.2 Contenu de la réponse

2.2.1 **Une réponse complète à la DRPE comprend ce qui suit** :

2.2.1.1 le **formulaire de présentation de la réponse à la DRPE des SII de l'annexe A, rempli** : Les répondants devraient inclure les renseignements contenus dans le formulaire de présentation de la réponse à la DRPE (annexe A) avec leurs réponses. Il s'agit d'un formulaire courant dans lequel les répondants peuvent fournir les renseignements exigés dans le cadre de l'évaluation, comme le nom d'une personne-ressource, le numéro d'entreprise – approvisionnement du fournisseur, le statut du fournisseur au titre du Programme de contrats fédéraux pour l'équité en matière d'emploi, etc. L'utilisation du formulaire pour fournir ces renseignements n'est pas obligatoire, mais recommandée. Si les renseignements exigés ne sont pas fournis dans la réponse à la DRPE, le répondant doit les fournir sur demande de l'autorité contractante;

2.2.1.2 la **liste des produits de TI de l'annexe C, remplie** : Les répondants doivent inclure une liste complète des produits de TI;

Remarque à l'intention des répondants : les répondants doivent utiliser l'annexe C de la DRPE pour présenter les renseignements exigés en 2.2.1.2 dans leur réponse.

2.2.1.3 **Schéma du réseau**

2.2.1.3.1 Les répondants doivent inclure un schéma du réseau qui comprend au minimum :

- 2.2.1.3.1.1 la topologie du réseau physique et logique illustrant les nœuds et les connexions entre les nœuds du réseau;
- 2.2.1.3.1.2 des détails sur les nœuds du réseau, les protocoles, les largeurs de bande, etc.;

2.2.1.4 **Attestations**



2.2.1.4.1 Les répondants doivent fournir les attestations exigées aux termes de la partie 5 de la DRPE.

2.3 Exigences relatives à la sécurité

2.3.1 L'entrepreneur doit, en tout temps au cours de l'exécution du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, être titulaire d'une cote de vérification d'organisation désignée (VOD), comprenant la sécurité de la technologie de l'information, délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur et ses employés doivent TOUS détenir une cote de fiabilité en vigueur, délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur doit posséder une autorisation de détenir des renseignements (ADR) valide, au niveau Protégé A, délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur et ses employés NE DOIVENT PAS emporter de renseignements ou des biens PROTÉGÉS B et C ou CLASSIFIÉS hors des lieux de travail précisés.

L'entrepreneur et ses employés NE DOIVENT PAS utiliser les systèmes de TI de l'entrepreneur pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS B et C ou CLASSIFIÉS.

Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de Services partagés Canada.

L'entrepreneur et ses employés doivent se conformer aux dispositions des textes suivants :

- a) Justice Canada – *Loi sur la protection de l'information* (dernière édition);
- b) Manuel de la sécurité industrielle (dernière édition).

2.4 Établissement des prix

2.4.1 Les renseignements sur les prix relatifs au besoin en SII ne sont pas compris dans la réponse à la présente DRPE.

Remarque à l'intention des répondants : La réponse fournie par le répondant retenu sera incorporée par renvoi à tout contrat subséquent et peut être incluse dans la clause sur l'ordre de priorité des documents de tout contrat subséquent.



PART 3 APERÇU DU PROCESSUS D'APPROVISIONNEMENT

3.1 Aperçu

- 3.1.1 L'étape de la DRPE est la première étape du processus en plusieurs étapes d'approvisionnement en SII résumé au tableau 1. La DRPE définit les exigences relatives à l'étape de la DP. L'objectif de l'étape de la DRPE est de sélectionner les répondants qualifiés (qui seront appelés « répondants retenus ») qui seront pris en considération dans le processus d'approvisionnement en SII.
- 3.1.2 Le 12 juillet 2012, Services partagés Canada a invoqué l'exception relative à la sécurité nationale (ESN) aux termes des accords commerciaux en ce qui concerne les approvisionnements relatifs aux services de courriel, aux réseaux et aux centres de données. Le présent besoin est donc soumis à une ESN.
- 3.1.3 Se reporter à la partie 4 pour une explication plus détaillée des procédures d'évaluation de la DRPE et de la sélection des répondants qualifiés.

Tableau 1 - Résumé du processus d'approvisionnement en SII

Étape d'approvisionnement	Objectifs
DRPE	<ul style="list-style-type: none">• Publier la DRPE par l'intermédiaire du Service électronique d'appels d'offres du gouvernement (MERX).• Obtenir des réponses à la DRPE.• Évaluer les réponses à la DRPE.• Sélectionner les répondants qualifiés afin de passer à la phase de la version provisoire de la DP.
DP	<ul style="list-style-type: none">• Envoyer la DP définitive à tous les répondants retenus.• Recevoir les réponses des soumissionnaires.• Évaluer les soumissions.
Attribution du contrat	<ul style="list-style-type: none">• Attribuer les contrats portant sur les SII aux soumissionnaires retenus.



PART 4 PROCÉDURES D'ÉVALUATION ET SÉLECTION DES RÉPONDANTS QUALIFIÉS

4.1 Procédures d'évaluation

- 4.1.1 Les réponses seront évaluées par rapport à l'ensemble des exigences de la DRPE.
- 4.1.2 Le processus d'évaluation de la DRPE est composé des deux étapes suivantes :
 - 4.1.2.1 étape 1 : évaluation de la liste des produits de TI;
 - 4.1.2.2 étape 2 : sélection des fournisseurs qualifiés.

4.2 Critères techniques obligatoires

On examinera chaque réponse pour déterminer si elle satisfait aux exigences obligatoires de la DRPE. Tous les éléments de la DRPE qui constituent des exigences obligatoires sont désignés par les termes « doit », « doivent » ou « obligatoire ». Les réponses qui ne respectent pas chacune des exigences obligatoires seront rejetées.

4.2.1 Les critères techniques obligatoires sont les suivants :

- 4.2.1.1 une liste des produits de TI conformément à l'annexe C;
- 4.2.1.2 un schéma complet du réseau, comme décrit en 2.2.1.3.

- 4.2.2 Le Canada aura le droit de demander des renseignements supplémentaires sur tout élément de la liste des produits de TI du répondant avant la publication de la DP. Le répondant disposera d'un (1) jour ouvrable (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir au Canada les renseignements nécessaires. Si ce délai n'est pas respecté, la réponse pourra être rejetée.
- 4.2.3 L'autorité contractante informera les répondants, par écrit, de l'approbation ou du rejet de leur liste de produits de TI. Si sa liste de produits de TI est approuvée, le répondant recevra une lettre d'approbation accompagnée d'une copie de la liste de produits de TI approuvée.
- 4.2.4 Si la liste de produits de TI du répondant n'est pas approuvée, le répondant disposera de dix (10) jours civils après la réception de l'avis écrit du Canada pour présenter une autre liste de produits de TI. Si la liste des produits de TI du répondant est rejetée une seconde fois, il n'y aura plus de possibilités de présenter une nouvelle liste de produits de TI. Le répondant ne sera pas retenu pour passer à la prochaine étape du processus d'approvisionnement.

4.3 Étape 2 : Sélection de répondants qualifiés

- 4.3.1 Une réponse doit respecter les exigences de la DRPE et satisfaire à tous les critères d'évaluation technique obligatoires pour être déclarée un fournisseur qualifié.



PART 5 ATTESTATIONS

Le Canada vérifie la conformité des attestations que les répondants lui ont fournies pendant la période d'évaluation des réponses et les étapes subséquentes du processus d'approvisionnement décrit dans la présente DRPE, et après l'attribution d'un marché. En tout temps avant l'attribution d'un marché, l'autorité contractante aura le droit de demander des renseignements supplémentaires pour s'assurer que les répondants respectent les attestations. La réponse du répondant sera rejetée et toute soumission présentée dans les étapes subséquentes sera déclarée non recevable si l'on constate que le répondant a fait de fausses déclarations, sciemment ou non. À défaut de respecter les attestations ou de donner suite à la demande de renseignements supplémentaires de l'autorité contractante, la soumission sera déclarée non recevable.

Les attestations suivantes doivent accompagner la réponse des répondants qui devrait être documentée à l'annexe A - formulaire de présentation de la DRPE des SII :

5.1 Programme de contrats fédéraux – Attestation

- 5.1.1 Conformément au Programme de contrats fédéraux pour l'équité en matière d'emploi (PCF EE), certains répondants, y compris un répondant qui est membre d'une coentreprise, qui présentent une soumission pour des marchés du gouvernement fédéral d'une valeur de 200 000 \$ ou plus (incluant toutes les taxes applicables) doivent s'engager officiellement à mettre en œuvre un programme d'équité en matière d'emploi. Il s'agit d'une condition préalable à l'attribution du contrat. Si le répondant est assujéti au Programme de contrats fédéraux (PCF), une preuve de son engagement doit accompagner sa réponse.
- 5.1.2 Les répondants qui ont été déclarés entrepreneurs non admissibles par Ressources humaines et Développement des compétences Canada (RHDC) n'ont plus le droit d'obtenir des contrats du gouvernement au-delà du seuil prévu par le Règlement sur les marchés de l'État pour les demandes de soumissions. Les répondants peuvent être déclarés entrepreneurs inadmissibles soit parce que RHDC a constaté leur non-conformité ou parce qu'ils se sont retirés volontairement du PCF pour une raison autre que la réduction de leur effectif à moins de 100 employés. Toute soumission présentée par un entrepreneur non admissible sera déclarée non recevable.
- 5.1.3 S'il n'est pas visé par les exceptions énumérées aux alinéas 5.1.4.1 ou 5.1.4.2 ci-après, ou qu'il n'a pas de numéro d'attestation valide confirmant son adhésion au PCF, le répondant doit télécopier (819-953-8768) un exemplaire signé du formulaire LAB 1168, Attestation d'engagement pour la mise en œuvre de l'équité en matière d'emploi, à la Direction générale du travail de RHDC.
- 5.1.4 On demande que chaque répondant indique dans sa soumission soit qu'il :
 - 5.1.4.1 n'est pas assujéti au PCF, puisqu'il compte un effectif de moins de 100 employés permanents à temps plein ou à temps partiel ou d'employés temporaires ayant travaillé au moins 12 semaines au Canada;
 - 5.1.4.2 n'est pas assujéti au Programme, puisqu'il est un employeur réglementé en vertu de la Loi sur l'équité en matière d'emploi, L.C. 1995, ch. 44;
 - 5.1.4.3 est assujéti aux exigences du PCF, puisqu'il compte un effectif d'au moins 100 employés permanents à plein temps ou à temps partiel ou d'employés temporaires ayant travaillé au moins 12 semaines ou plus au Canada, mais n'a pas obtenu de numéro d'attestation de RHDC (puisque'il n'a jamais soumissionné de marchés de 200 000 \$ ou plus). Dans ce cas, une attestation d'engagement dûment signée est exigée;
 - 5.1.4.4 est assujéti au PCF et possède un numéro d'attestation valide (c.-à-d. qu'il n'a pas été déclaré entrepreneur non admissible par RHDC).
- 5.1.5 Des renseignements supplémentaires sur le PCF sont offerts sur le site Web de RHDC, à l'adresse suivante : <http://www.rhdcc.gc.ca/fr/passerelles/topiques/wzp-gxr.shtml>.



Remarque à l'intention des répondants : Les répondants doivent utiliser le formulaire de présentation de la réponse à la DRPE des SII (annexe A) pour fournir les renseignements concernant leur état aux termes de ce programme. Dans le cas d'un répondant faisant partie d'une coentreprise, ces renseignements doivent être fournis pour chaque membre de la coentreprise.

5.2 Attestation pour ancien fonctionnaire

- 5.2.1 Les marchés attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats avec d'anciens fonctionnaires, les répondants doivent fournir les renseignements exigés ci-après.
- 5.2.2 Aux fins de la présente clause :
- 5.2.2.1 « **ancien fonctionnaire** » signifie un ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques*, L.R., 1985 ch. F-11, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :
- 5.2.2.1.1 un individu;
 - 5.2.2.1.2 un individu qui s'est incorporé;
 - 5.2.2.1.3 une société de personnes constituée d'anciens fonctionnaires; ou
 - 5.2.2.1.4 une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.
- 5.2.2.2 « **période du paiement forfaitaire** » désigne la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'allocation de fin de services, qui se mesure de façon similaire.
- 5.2.2.3 « **pension** » signifie, dans le contexte de la formule de réduction des honoraires, une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension dans la fonction publique* (LPFP), L.R., 1985, ch. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17, à la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3, à la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada*, 1970, ch. R-10, et à la *Loi sur la pension de retraite de la Gendarmerie royale du Canada*, L.R., 1985, ch. R-11, à la *Loi sur les allocations de retraite des parlementaires* L.R., 1985, ch. M-5, et à la partie de la pension versée conformément à la *Loi sur le Régime de pensions du Canada*, L.R., 1985, ch. C-8.
- 5.2.3 Si le répondant est un ancien fonctionnaire touchant une pension, selon la définition qui en est donnée ci-dessus, il doit fournir l'information suivante :
- 5.2.3.1 le nom de l'ancien fonctionnaire;
 - 5.2.3.2 la date de cessation d'emploi dans la fonction publique ou de la retraite.
- 5.2.4 S'il est un ancien fonctionnaire qui a reçu un paiement forfaitaire conformément aux dispositions d'un programme de réduction des effectifs, le répondant doit fournir l'information suivante :
- 5.2.4.1 le nom de l'ancien fonctionnaire;
 - 5.2.4.2 les conditions de l'incitatif versé sous forme de paiement forfaitaire;
 - 5.2.4.3 la date de la cessation d'emploi dans la fonction publique;
 - 5.2.4.4 le montant du paiement forfaitaire;
 - 5.2.4.5 le taux de rémunération qui a servi au calcul du paiement forfaitaire;



- 5.2.4.6 la période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines;
- 5.2.4.7 le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réduction des effectifs.
- 5.2.5 Pour tous les marchés attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peut être payé à un ancien fonctionnaire qui a reçu un paiement forfaitaire est limité à 5 000 \$, incluant la taxe sur les produits et services ou la taxe de vente harmonisée.
- 5.2.6 En déposant une réponse, le répondant atteste que les renseignements fournis pour répondre aux exigences énoncées plus haut sont exacts et complets.

Remarque à l'intention des répondants : On demande aux répondants d'utiliser le formulaire de présentation de leur réponse (annexe A) pour fournir les renseignements demandés par la présente clause.

ANNEXE A

FORMULAIRE DE PRÉSENTATION DE LA RÉPONSE À LA DRPE		
DRPE N° : 10026415/A		
Dénomination sociale complète du répondant : [Remarque à l'intention des répondants : Il incombe aux répondants qui font partie d'une entreprise de désigner la bonne entreprise.]		
Représentant autorisé du répondant aux fins d'évaluation (p. ex., pour des précisions)	Nom	
	Titre	
	Adresse	
	Téléphone	
	Télécopieur	
	Courriel	
Numéro d'entreprise – approvisionnement (NEA) du répondant [voir la clause 2003 des instructions et conditions uniformisées] [Remarque à l'intention des répondants : Le NEA donné doit correspondre à la dénomination sociale utilisée dans la soumission. Si ce n'est pas le cas, on établira le répondant en fonction de la dénomination sociale fournie, et le répondant devra donner le NEA qui correspond à celle-ci.]		
Autorité compétente : La province du Canada choisie par le répondant qui aura les compétences sur tout contrat subséquent (si différente de celle précisée dans la demande)		
Langue officielle du Canada utilisée par le fournisseur pour communiquer avec le Canada – indiquer le français ou l'anglais		
Anciens fonctionnaires Voir l'article de la partie 5 de la demande de soumissions intitulée Attestation pour ancien fonctionnaire pour la définition de « ancien fonctionnaire ».	<p>Le répondant est-il un ancien fonctionnaire touchant une pension tel que le définit la demande de soumissions?</p> <p>Oui ____ Non ____</p> <p>Si oui, fournir les renseignements demandés par l'article de la partie 5 intitulé « Attestation pour ancien fonctionnaire ».</p>	

FORMULAIRE DE PRÉSENTATION DE LA RÉPONSE À LA DRPE

DRPE N° : 10026415/A

	<p>Le répondant est-il un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu des dispositions d'un programme de réduction des effectifs?</p> <p>Oui ____ Non ____</p> <p>Si oui, fournir les renseignements demandés par l'article de la partie 5 intitulé « Attestation pour ancien fonctionnaire ».</p>	
<p>Attestation du Programme de contrats fédéraux pour l'équité en matière d'emploi (PCF EE) :</p> <p>Si le répondant n'y est pas assujéti, en indiquer la raison à droite. S'il ne satisfait à aucune des conditions énoncées dans la colonne de droite, il est tenu, en vertu des exigences du programme, de :</p> <p>a) remettre au ministère des Ressources humaines et du Développement des compétences (RHDC) le formulaire LAB1168, Attestation d'engagement pour la mise en œuvre de l'équité en matière d'emploi, DUMENT SIGNÉ; ou</p> <p>(b) fournir un numéro d'attestation valide pour confirmer son adhésion au PCF.</p> <p>On demande aux répondants de joindre à leur soumission leur attestation au PCF ou le formulaire LAB 1168 signé; si cette information n'accompagne pas la soumission, elle doit être fournie sur demande de l'autorité contractante durant l'évaluation.</p> <p>Dans le cas d'une coentreprise, veuillez fournir ces renseignements pour chacun des membres de la coentreprise.</p>	<p>En apposant ma signature ci-après, j'atteste également, au nom du répondant, que ce dernier [cocher la case appropriée]:</p>	
	<p>a) n'est pas assujéti aux exigences du programme, puisqu'il compte un effectif de moins de 100 employés permanents à temps plein ou à temps partiel;</p>	
	<p>b) n'est pas assujéti au programme, puisqu'il est un employeur réglementé en vertu de la <i>Loi sur l'équité en matière d'emploi</i>;</p>	
	<p>c) est assujéti aux exigences du Programme, puisqu'il compte un effectif de 100 employés permanents ou plus à temps plein ou à temps partiel au Canada, mais il n'a pas obtenu auparavant un numéro d'attestation du ministère des Ressources humaines et du Développement des compétences (RHDC) (n'ayant pas soumissionné des marchés de 200 000 \$ ou plus); dans ce cas, un certificat d'engagement dûment signé est joint à la présente);</p>	

FORMULAIRE DE PRÉSENTATION DE LA RÉPONSE À LA DRPE

DRPE N° : 10026415/A

d) est assujetti au programme et possède un numéro d'attestation valide, à savoir le numéro : _____ (et il n'a pas été déclaré entrepreneur non admissible par RHDC).

Nombre d'ETP [On demande aux répondants d'indiquer le nombre total de postes équivalents à temps plein (ETP) qu'ils devront créer et conserver si le marché leur était adjugé. Ce renseignement n'est demandé qu'à titre indicatif et ne sera pas pris en compte dans l'évaluation.]

Niveau d'attestation de sécurité du répondant

[indiquer le niveau et la date d'attribution]

[Note à l'intention des répondants : assurez-vous que le nom dans l'attestation de sécurité correspond à la dénomination sociale du répondant. Si ce n'est pas le cas, l'attestation n'est pas valide pour le répondant.]

En tant que PDG du fournisseur, en apposant ma signature ci-dessous, j'atteste que j'ai lu et compris la DRPE en entier, y compris les documents incorporés par renvoi dans la DRPE et dans l'ensemble de la réponse, et que :

1. que tous les renseignements fournis dans la réponse à la DRPE sont exacts et complets.

**Signature du représentant autorisé du
répondant**



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE			
1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine Shared Services Canada		2. Branch or Directorate / Direction générale ou Direction Transformation and Services Strategy Design	
3. a) Subcontract Number / Numéro du contrat de sous-traitance		3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant	
4. Brief Description of Work / Brève description du travail Internet Interconnect Services (IIS), to replace diverse and redundant Internet services under the expiring SCNet contracts.			
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?		<input checked="" type="checkbox"/> No / Non	<input type="checkbox"/> Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?		<input checked="" type="checkbox"/> No / Non	<input type="checkbox"/> Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis			
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)		<input type="checkbox"/> No / Non	<input checked="" type="checkbox"/> Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.		<input checked="" type="checkbox"/> No / Non	<input type="checkbox"/> Yes / Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?		<input checked="" type="checkbox"/> No / Non	<input type="checkbox"/> Yes / Oui
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès			
Canada <input checked="" type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	Foreign / Étranger <input type="checkbox"/>	
7. b) Release restrictions / Restrictions relatives à la diffusion			
No release restrictions / Aucune restriction relative à la diffusion <input checked="" type="checkbox"/>	All NATO countries / Tous les pays de l'OTAN <input type="checkbox"/>	No release restrictions / Aucune restriction relative à la diffusion <input type="checkbox"/>	
Not releasable / À ne pas diffuser <input type="checkbox"/>			
Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	
Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:	
7. c) Level of information / Niveau d'information			
PROTECTED A / PROTÉGÉ A <input checked="" type="checkbox"/>	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A / PROTÉGÉ A <input type="checkbox"/>	
PROTECTED B / PROTÉGÉ B <input type="checkbox"/>	NATO RESTRICTED / NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B / PROTÉGÉ B <input type="checkbox"/>	
PROTECTED C / PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL / NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C / PROTÉGÉ C <input type="checkbox"/>	
CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/>	NATO SECRET / NATO SECRET <input type="checkbox"/>	CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/>	
SECRET / SECRET <input type="checkbox"/>	COSMIC TOP SECRET / COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET / SECRET <input type="checkbox"/>	
TOP SECRET / TRÈS SECRET <input type="checkbox"/>		TOP SECRET / TRÈS SECRET <input type="checkbox"/>	
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/>	



Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? No / Non Yes / Oui
Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

- | | | | |
|---|---|---|--|
| <input checked="" type="checkbox"/> RELIABILITY STATUS
COTE DE FIABILITÉ | <input type="checkbox"/> CONFIDENTIAL
CONFIDENTIEL | <input type="checkbox"/> SECRET
SECRET | <input type="checkbox"/> TOP SECRET
TRÈS SECRET |
| <input type="checkbox"/> TOP SECRET - SIGINT
TRÈS SECRET - SIGINT | <input type="checkbox"/> NATO CONFIDENTIAL
NATO CONFIDENTIEL | <input type="checkbox"/> NATO SECRET
NATO SECRET | <input type="checkbox"/> COSMIC TOP SECRET
COSMIC TRÈS SECRET |
| <input type="checkbox"/> SITE ACCESS
ACCÈS AUX EMPLACEMENTS | | | |

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE: Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No / Non Yes / Oui
If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté? No / Non Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? No / Non Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? No / Non Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? No / Non Yes / Oui



Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

PART C - (continued) / PARTIE C - (suite)

For users completing the form manually use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire manuellement doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC						
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ			CONFIDENTIAL	SECRET	TOP SECRET	
				CONFIDENTIEL	TRÈS SECRET	NATO DIFFUSION RESTREINTE	NATO CONFIDENTIEL		A		B	C	CONFIDENTIEL		TRÈS SECRET		
Information / Assets Renseignements / Biens Production	✓																
IT Media / Support TI	✓																
IT Link / Lien électronique	✓																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED? No / Yes
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? Non / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED? No / Yes
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? Non / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

ANNEXE D - DRAFT DEMANDE DE SOUMISSIONS POUR LE SERVICES D'INTERCONNEXION INTERNET POUR SERVICES PARTAGÉS CANADA

TABLE DES MATIÈRES

PART 1 RENSEIGNEMENTS GÉNÉRAUX.....	3
1.1 Introduction.....	3
1.2 Sommaire	3
1.3 Comptes rendus	4
PART 2 INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES	5
2.1 Instructions, clauses et conditions uniformisées.....	5
2.2 Présentation des soumissions.....	6
2.3 Lois applicables.....	6
2.4 Demandes de renseignements.....	6
PART 3 INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....	7
3.1 Instructions pour la préparation des soumissions.....	7
3.2 Section I : Soumission technique.....	7
3.3 Section II : Soumission financière.....	8
3.4 Section III : Attestations.....	9
3.5 Fluctuation du taux de change.....	9
PART 4 PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION.....	10
4.1 Procédures d'évaluation	10
4.2 Évaluation technique – Critères obligatoires de l'évaluation technique	10
4.3 Évaluation financière.....	11
4.4 Méthode de sélection	11
PART 5 ATTESTATIONS	11
5.1 Attestations exigées dans les Instructions uniformisées supplémentaires 2003-1	12
5.2 Attestation pour le Code de conduite.....	12
PART 6 EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES	13
6.1 Exigences relatives à la sécurité	13
6.2 Capacité financière.....	13
PART 7 CLAUSES DU CONTRAT SUBSÉQUENT	14
7.1 Exigence	14
7.2 Commandes de services.....	15
7.3 Processus de commande de services.....	15

7.4	Modification à la commande de services	17
7.5	Garantie des travaux minimaux	17
7.6	Clauses et conditions uniformisées	18
7.7	Exigences relatives à la sécurité	18
7.8	Sécurité de la chaîne d'approvisionnement	23
7.9	Durée du contrat	23
7.10	Responsables	24
7.11	Paiement	24
7.12	Instructions relatives à la facturation	29
7.13	Attestations	29
7.14	Lois applicables	29
7.15	Ordre de priorité des documents	29
7.16	Ressortissants étrangers (entrepreneur canadien)	30
7.17	Ressortissants étrangers (entrepreneur étranger)	30
7.18	Exigences en matière d'assurance	30
7.19	Limitation de la responsabilité – Gestion de l'information et de la technologie de l'information	30
7.20	Entrepreneur en coentreprise	32
7.21	Services de télécommunications	32
7.22	Mise en place des installations de télécommunications dans les immeubles du Canada	32
7.23	Préservation des supports électroniques	33
7.24	Déclarations et garanties	33
7.25	Services de transition à la fin de la période visée par le contrat	33

Liste des annexes du contrat subséquent :

Annexe A	Énoncé des travaux
Annexe B	Prix des Services d'interconnexion Internet (SII)
Annexe C	Liste de vérification des exigences relatives à la sécurité
Annexe D	Accès aux biens de l'État pour les services de télécommunications
Annexe E	Format du fichier de facturation

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

Pièce jointe 4.1 : Critères obligatoires de l'évaluation technique
Pièce jointe 4.2 : Classeur d'évaluation des prix

Formulaires : Formulaire 1 – Formulaire de présentation de la soumission

DEMANDE DE SOUMISSIONS POUR SERVICES D'INTERCONNEXION INTERNET POUR SERVICES PARTAGÉS CANADA

PART 1 RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

L'invitation à soumissionner contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 – Renseignements généraux : renferme une description générale du besoin;

Partie 2 – Instructions à l'intention des soumissionnaires : instructions, clauses et conditions relatives à l'invitation à soumissionner;

Partie 3 – Instructions de préparation d'une soumission : instructions sur la manière de préparer une soumission;

Partie 4 Procédures d'évaluation et méthode de sélection : décrivent la façon selon laquelle se déroulera l'évaluation et présentent les critères d'évaluation auxquels le soumissionnaire doit répondre dans la soumission, s'il y a lieu, ainsi que la méthode de sélection;
Pièce jointe 4.1 - Critères d'évaluation technique obligatoires
Pièce jointe 4.2 : Classeur d'évaluation des prix

Partie 5 Attestations : décrivent les attestations à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences : description des exigences particulières auxquelles le soumissionnaire doit répondre;

Partie 7 Clauses du contrat subséquent : clauses et conditions qui s'appliqueront à tout contrat subséquent, ainsi que les annexes suivantes :

Annexe A - Énoncé des travaux

Annexe B – Prix des SII

Annexe C – Liste de vérification des exigences relatives à la sécurité

Annexe D – Accès aux biens de l'État pour les services de télécommunications

Annexe E – Format du fichier de facturation

1.2 Sommaire

Services partagés Canada (SPC) a besoin d'un service d'interconnexion Internet (SII) diversifié qui lui permettra d'accéder aux services Internet publics, tout en contribuant à la prestation des programmes et des services offerts aux Canadiens par d'autres ministères et organismes.

Les services suivants constituent le besoin en matière de SII et seront fournis au besoin :

- services d'interconnexion Internet (SII);
- service de protection contre les attaques par déni de service distribué (DDOS);
- déplacement de circuits;
- tout produit livrable requis conformément au contrat.

Les services ci-dessus seront fournis dans la région de la capitale nationale (RCN) et dans la région de Toronto (TOR), au Canada, à l'exclusion de tout lieu se trouvant dans des zones visées par les Ententes sur les revendications territoriales globales.

Le besoin est constitué de trois points d'interface de service (PIS) redondants pour les SII, devant être fournis par deux ou trois entrepreneurs distincts, dont deux dans la RCN et un dans la région de Toronto; où chaque PIS aura la capacité et la fiabilité nécessaires pour gérer tout le trafic Internet en cas de défaillance des autres PIS.

SPC se servira des marchés subséquents pour fournir des services partagés à ses clients, soit lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant le marché, et les autres organisations qui choisissent de recourir à ses services de temps en temps, à tout moment pendant le marché. La présente demande de soumissions vise à aboutir à l'attribution de deux ou de trois contrats, chacun pour une période de 3 ans, plus une option irrévocable d'un an (1) qui permet au Canada de prolonger la durée du contrat.

Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples informations, voir la partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la partie 7, Clauses du contrat subséquent. Les soumissionnaires devraient consulter le document « Exigences de sécurité dans les demandes de soumissions de TPSGC – Instructions pour les soumissionnaires » (<http://www.tpsgc.gc.ca/acquisitions/text/plain/plain-f.html#top>) sur le site Web des documents uniformisés d'approvisionnement du ministère.

Le 12 juillet 2012, Services partagés Canada a invoqué l'exception au titre de la sécurité nationale en vertu des accords commerciaux, pour ce qui est des marchés relatifs aux courriels, aux réseaux et aux centres de données pour Services partagés Canada. Le présent besoin est donc soumis à une exception au titre de la sécurité nationale.

1.3 Comptes rendus

Après l'attribution du contrat, les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires doivent en faire la demande à l'autorité contractante dans les quinze (15) jours ouvrables suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

PART 2 INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

- 2.1.1 Toutes les instructions, clauses et conditions de la demande de soumissions sont identifiées par un numéro, une date et un titre dans le Guide des clauses et conditions uniformisées d'achat (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>), produit par Travaux publics et Services gouvernementaux Canada.
- 2.1.2 Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003 (2012-11-19) Instructions uniformisées - biens ou services – besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante. En cas de divergence entre les dispositions du document 2003 et ce document, ce dernier l'emporte.

Toutes les références à Travaux publics et Services gouvernementaux Canada (TPSGC) contenues dans les Instructions uniformisées seront interprétées comme une référence à SPC.

Le texte du paragraphe 4 de la section 01 – Code de conduite et attestations, du document 2003 susmentionné est remplacé par ce qui suit :

Les soumissionnaires doivent fournir avec leur soumission, ou le plus tôt possible après l'avoir déposée, une liste complète des personnes qui occupent actuellement un poste d'administrateur au sein de leur entreprise. Si la liste n'a pas été fournie à la fin de l'évaluation des soumissions, le Canada informera les soumissionnaires du délai dans lequel l'information doit être fournie. Si cette liste n'est pas fournie dans le délai prescrit, la soumission sera déclarée irrecevable. Les soumissionnaires doivent toujours fournir la liste des administrateurs avant l'attribution du marché.

Le Canada peut, en tout temps, demander aux répondants de fournir dans un délai donné un formulaire de consentement dûment rempli et signé ([Consentement à la vérification de l'existence d'un casier judiciaire](#) [PWGSC-TPSGC 229]) pour les personnes inscrites sur la liste susmentionnée. Si le soumissionnaire ne fournit pas le formulaire de consentement dans le délai prescrit, sa soumission sera déclarée irrecevable.

Le texte du paragraphe 5 de la section 01 – Code de conduite et attestations, du document 2003 susmentionné est remplacé par ce qui suit :

Le soumissionnaire doit diligemment tenir à jour la liste en informant le Canada, par écrit, de tout changement survenant au cours de la période de validité de la soumission. Il doit également fournir au Canada les formulaires de consentement correspondants, au besoin. En outre, le soumissionnaire devra diligemment tenir à jour la liste et fournir, au besoin, les formulaires de consentement au cours de la période d'exécution de tout contrat découlant de la présente invitation à soumissionner.

- 2.1.3 La section 3 des Instructions uniformisées – biens et services – besoins concurrentiels 2003 est modifiée comme suit : supprimer « conformément à la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*, L.C. 1996, ch. 16 ».
- 2.1.4 Le paragraphe 5(4) du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels est modifié comme suit :
- Supprimer : soixante (60) jours
- Insérer : cent vingt (120) jours
- 2.1.5 Les Instructions uniformisées – biens et services – besoins concurrentiels 2003 sont modifiées comme suit : supprimer la section 8, Transmission par télécopieur, en entier.

- 2.1.6 Les Instructions uniformisées supplémentaires – télécommunications 2003-1 (2008-05-12) sont incorporées par renvoi à la demande de soumissions et en font partie intégrante. S'il y a un conflit entre les dispositions des instructions 2003-1 et le présent document, ce dernier l'emporte.

2.2 Présentation des soumissions

- 2.2.1 Les soumissions doivent être présentées uniquement à Services partagés Canada au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.
- 2.2.2 En raison de la nature de la demande de soumissions, les soumissions transmises par télécopieur à SPC ne seront pas acceptées.

2.3 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur en Ontario, et les relations entre les parties seront déterminées par ces lois.

Remarque à l'intention des soumissionnaires : Un soumissionnaire peut, à sa discrétion, indiquer les lois applicables d'une province ou d'un territoire canadien de son choix, sans que la validité de sa soumission ne soit remise en question, en supprimant le nom de la province ou du territoire canadien précisé et en le remplaçant par celui de la province ou du territoire de son choix. *Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées. On demande aux soumissionnaires d'indiquer, dans le Formulaire de présentation de la soumission, la province ou le territoire canadien dans lequel ils souhaitent obtenir tout contrat subséquent.*

2.4 Demandes de renseignements

- 2.4.1 Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 10 jours civils avant la date de clôture de la demande de soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.
- 2.4.2 Les soumissionnaires doivent citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question. Ils doivent prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec précision. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les soumissionnaires.
- 2.4.3 Le Canada ne répondra pas aux questions relatives à l'énoncé des travaux (EDT) au cours de la phase de demande de soumissions (DP) du processus d'approvisionnement.. Il répondra plutôt aux questions à la phase de la demande de réponses pour l'évaluation (DRPE).

PART 3 INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

3.1.1 Copies de la soumission : Le Canada demande aux soumissionnaires de présenter une soumission dont les sections sont reliées séparément, comme suit :

3.1.1.1 Section I : Soumission technique (une version papier finale et trois copies papier) et deux copies électroniques sur CD ou DVD).

3.1.1.2 Section II : Soumission financière (une version papier finale) et une copie électronique sur CD ou DVD).

3.1.1.3 Section III : Attestations (une version papier finale).

3.1.1.4 En cas d'incompatibilité entre le libellé de la copie électronique et de l'exemplaire papier, le libellé de l'exemplaire papier l'emportera.

3.1.1.5 En cas d'incompatibilité entre le libellé de n'importe laquelle des copies, le libellé de la version finale l'emportera sur celui de la copie.

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

3.1.2 Format de la soumission : Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-après pour préparer leur soumission :

3.1.2.1 utiliser du papier 8,5 po x 11 po (216 mm x 279 mm);

3.1.2.2 utiliser un système de numérotation correspondant à celui de la demande de soumissions :

3.1.2.3 joindre une page titre sur chaque volume de la soumission comprenant le titre, la date, le numéro de la demande de soumissions, le nom et l'adresse du soumissionnaire et les coordonnées de son représentant;

3.1.2.4 joindre une table des matières.

3.1.3 Politique d'achats écologiques du Canada : En avril 2006, le Canada a approuvé une politique exigeant que les organismes et ministères fédéraux prennent les mesures nécessaires pour incorporer les facteurs environnementaux dans le processus d'approvisionnement. Veuillez consulter la Politique d'achats écologiques (<http://tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html>). Pour aider le Canada à atteindre ses objectifs, on encourage les soumissionnaires à faire ce qui suit :

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

3.1.3.2 utiliser un format qui respecte l'environnement : impression noir et blanc plutôt que couleur, impression recto verso, et des agrafes ou des trombones plutôt qu'une reliure Cerlox, une reliure à attaches ou une reliure à anneaux.

3.2 Section I : Soumission technique

3.2.1 Dans leur soumission technique, les soumissionnaires doivent montrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils y répondront. Les soumissionnaires doivent démontrer leur capacité et décrire l'approche qu'ils prendront de façon complète, concise et claire pour effectuer les travaux. La soumission technique doit traiter, de façon claire et suffisamment détaillée, les points visés par les critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Pour faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

3.2.2 La soumission technique comprend ce qui suit :

3.2.2.1 Formulaire de présentation de la soumission (Formulaire 1) : Les soumissionnaires doivent joindre le formulaire de présentation de la soumission à leurs soumissions. Il s'agit d'un formulaire commun dans lequel les soumissionnaires peuvent fournir les renseignements exigés dans le cadre de l'évaluation et de l'attribution du contrat, comme le nom d'une personne-ressource, le numéro d'entreprise - approvisionnement (NEA) du soumissionnaire, etc. L'utilisation du formulaire pour fournir ces renseignements n'est pas obligatoire, mais recommandée. Si le Canada considère que les renseignements demandés dans le formulaire de présentation des soumissions sont incomplets ou doivent être corrigés, il donnera au soumissionnaire la possibilité de les compléter ou de les corriger.

3.2.2.2 Pièce jointe 4.1 - Critères d'évaluation technique obligatoires

Dans la soumission technique, on doit présenter une justification selon laquelle le soumissionnaire et la solution qu'il propose sont conformes aux critères particuliers définis à la pièce jointe 4.1, document qui représente le format demandé pour fournir la justification. La pièce jointe sur les critères d'évaluation technique obligatoires n'est pas nécessaire pour remplir les parties de cette demande de soumissions qui ne sont pas mentionnées dans la pièce jointe. La justification ne doit pas être une simple répétition du besoin, mais doit expliquer et démontrer la façon dont le soumissionnaire satisfera aux exigences et exécutera les travaux exigés. Il n'est pas suffisant de simplement déclarer que le soumissionnaire, ou la solution ou les produits qu'il propose, est conforme. Si le Canada détermine que la justification n'est pas complète, le soumissionnaire sera jugé non conforme et sa soumission sera rejetée. La justification devrait mentionner des documents supplémentaires joints à la soumission. Cette information peut être mentionnée dans la colonne « Référence » de la pièce jointe 4.1, où les soumissionnaires doivent inclure l'endroit précis, dans leur soumission, où se trouvent les documents d'accompagnement, y compris le titre du document et les numéros de page et d'alinéa. Lorsque la référence n'est pas suffisamment précise, le Canada peut demander que le soumissionnaire lui indique l'endroit approprié dans le document.

3.2.2.3 Lettre d'approbation pour les produits de technologies de l'information (TI)

Les soumissionnaires doivent inclure la lettre qu'ils ont reçue du Canada à l'issue de leur réponse à la DRPE n° 10026415/A.

3.3 Section II : Soumission financière

3.3.1 Établissement des prix : Les soumissionnaires doivent présenter leur soumission financière conformément à la pièce jointe 4.2 – Classeur d'évaluation des prix. Le montant total de la taxe sur les produits et services, de la taxe de vente du Québec ou de la taxe de vente harmonisée doit être indiqué séparément, s'il y a lieu. Sauf indication contraire, les soumissionnaires doivent inclure un seul prix ferme, tout compris, en dollars canadiens, dans chaque cellule des tableaux de prix où il faut saisir des données.

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

3.3.3 Prix nuls : On demande aux soumissionnaires d'entrer « 0,00 \$ » pour tout article qu'ils ne comptent pas facturer ou qui a déjà été ajouté à d'autres prix dans les tableaux. Si le soumissionnaire laisse le champ vierge, le Canada considérera le prix comme étant « 0,00 \$ » aux fins d'évaluation et pourrait demander que le soumissionnaire confirme que le prix est bel et bien 0.00 \$. Aucun soumissionnaire ne sera autorisé à ajouter ou à modifier un prix durant cette confirmation. Si le soumissionnaire refuse de confirmer que le prix d'un champ en blanc est de « 0,00 \$ », sa soumission sera déclarée irrecevable.

3.4 Section III : Attestations

Les soumissionnaires doivent présenter les attestations exigées à la partie 5.

3.5 Fluctuation du taux de change

L'exigence ne prévoit aucune protection relative à la fluctuation du taux de change. Aucune demande de protection contre la fluctuation du taux de change ne sera prise en considération et une telle demande rendra la soumission irrecevable.

PART 4 PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

- 4.1.1 Les soumissions seront évaluées conformément à l'ensemble des exigences de la demande de soumissions, y compris les critères d'évaluation. Le processus d'évaluation comporte plusieurs étapes décrites ci-après. Même si l'évaluation et la sélection se déroulent par étapes, ce n'est pas parce que le Canada passe à une étape ultérieure qu'il a décidé que le soumissionnaire a réussi toutes les étapes antérieures. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.
- 4.1.2 Une équipe d'évaluation composée de représentants de SPC évaluera les soumissions. Le Canada peut faire appel à des experts-conseils indépendants ou à toute ressource gouvernementale pour évaluer les soumissions. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation.
- 4.1.3 En plus de tout autre délai établi dans la demande de soumissions :
- 4.1.3.1 **Demande de précisions** : Si le Canada demande au soumissionnaire de préciser certains aspects de sa soumission, ou s'il veut la vérifier, le soumissionnaire a deux jours ouvrables (ou plus si l'autorité contractante le précise par écrit) pour fournir les renseignements demandés. À défaut de respecter ce délai, sa soumission sera jugée non recevable.
- 4.1.3.2 **Demandes de renseignements supplémentaires** : Si le Canada a besoin de renseignements supplémentaires conformément à la section intitulée « Déroulement de l'évaluation » du document 2003, Instructions uniformisées - biens ou services - besoins concurrentiels, en vue de :
- 4.1.3.2.1 vérifier tout renseignement fourni par le soumissionnaire dans sa soumission;
- 4.1.3.2.2 **communiquer avec toute personne citée en référence pour vérifier et valider l'exactitude des renseignements fournis par le soumissionnaire;**

le soumissionnaire doit fournir les renseignements demandés dans les trois (3) jours ouvrables suivant la demande par l'autorité contractante.

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

4.2 Évaluation technique – Critères obligatoires de l'évaluation technique

- 4.2.1 On examinera chaque soumission pour déterminer si elle satisfait aux exigences obligatoires de la demande de soumissions. Tous les éléments de la demande de soumissions qui constituent des exigences obligatoires sont désignés par les termes « doit », « doivent » ou « obligatoire ». Les soumissions qui ne respectent pas l'ensemble des exigences obligatoires seront déclarées non recevables et rejetées.
- 4.2.2 Si une soumission énonce qu'une version ultérieure d'un produit qu'elle cite satisfera aux exigences obligatoires de la demande de soumissions, et que cette version ultérieure n'est pas disponible à la date de clôture des soumissions, la soumission sera rejetée.
- 4.2.3 Les exigences obligatoires sont décrites à la pièce jointe 4.1 – Critères obligatoires de l'évaluation technique.
- 4.2.4 **Démonstration**
- 4.2.4.1 Le Canada se réserve le droit, sans y être obligé, de demander que le soumissionnaire classé au premier rang (établi après l'évaluation financière) fasse une démonstration des caractéristiques, de la fonctionnalité et des capacités décrites dans la demande de soumissions ou dans sa soumission, afin d'en vérifier la conformité aux exigences de cette demande. Si une démonstration est exigée, elle doit être effectuée, sans frais pour le Canada, dans un endroit au Canada convenu avec l'autorité contractante. Le Canada donnera un avis d'au moins dix jours ouvrables avant la tenue de cette démonstration. La

démonstration devra se faire durant les heures normales de travail déterminées par l'autorité contractante. Le Canada paiera le coût salarial et les frais de déplacement qu'il aura engagés relativement à toute démonstration. Malgré la soumission écrite, si le Canada détermine pendant une démonstration que la solution proposée par le soumissionnaire ne satisfait pas aux exigences obligatoires de cette demande de soumissions, la soumission sera déclarée irrecevable.

4.3 Évaluation financière

4.3.1 L'évaluation financière sera effectuée en calculant le prix évalué global de la soumission pour la RCN et le prix évalué global de la soumission pour la région de Toronto, à l'aide des tableaux des prix remplis par les soumissionnaires qui se trouvent à la pièce jointe 4.2.

4.3.2 Formules figurant dans les tableaux d'établissement des prix

Si les tableaux d'établissement des prix fournis aux soumissionnaires ne comprennent aucune formule, le Canada peut entrer les prix fournis par les soumissionnaires dans un nouveau tableau, s'il estime que la formule ne fonctionne plus correctement selon la version fournie par le soumissionnaire.

4.4 Méthode de sélection

4.4.1 Une soumission qui respecte les exigences de la demande de soumissions et qui satisfait à tous les critères d'évaluation obligatoires sera déclarée conforme.

Les deux soumissions recevables dont le prix évalué global de la soumission est le plus bas pour la RCN seront recommandées pour l'attribution d'un contrat. Dans le cas où ces deux soumissions recevables n'affichent pas le prix évalué global de la soumission le plus bas pour la région de Toronto, la soumission recevable dont le prix évalué global de la soumission est le plus bas pour la région de Toronto sera également recommandée pour l'attribution d'un contrat.

4.4.2 Les soumissionnaires devraient prendre note que toutes les attributions de contrats sont assujetties au processus d'approbation interne du Canada, qui comprend une exigence relative à l'approbation du financement de tout contrat proposé. Même si un soumissionnaire a été recommandé en vue de l'attribution du contrat, le contrat ne sera accordé que si le processus interne correspond à la recommandation conformément aux politiques internes du Canada. Si l'approbation n'est pas obtenue, aucun marché ne sera adjugé.

PART 5 ATTESTATIONS

Pour qu'un contrat leur soit attribué, les soumissionnaires doivent fournir les attestations exigées. Le Canada déclarera une soumission non recevable si les attestations exigées ne sont pas remplies et fournies, tel qu'il est demandé.

Le Canada pourra vérifier l'authenticité des attestations fournies par les soumissionnaires, et cela comprend les attestations fournies à la phase de la DRPE, pendant la période d'évaluation des soumissions (avant l'attribution d'un contrat) et après l'attribution du contrat. L'autorité contractante aura le droit de demander des renseignements supplémentaires pour s'assurer que les soumissionnaires respectent les exigences en matière d'attestations avant l'attribution d'un marché. La soumission sera déclarée irrecevable si l'on constate que le soumissionnaire a fait de fausses déclarations, sciemment ou non. Le fait de ne pas respecter les exigences visant les attestations ou de ne pas donner suite à la demande de renseignements supplémentaires de l'autorité contractante aura pour effet de rendre la soumission irrecevable.

Les attestations énumérées ci-dessous devraient être remplies et fournies avec la soumission, mais elles peuvent être fournies plus tard. Si l'une de ces attestations n'est pas remplie et fournie comme demandé, l'autorité contractante en informera le soumissionnaire et lui donnera un délai afin de se conformer aux exigences. Le défaut de répondre à la demande de l'autorité contractante et de se conformer aux exigences dans les délais prévus aura pour conséquence que la soumission sera déclarée irrecevable.

5.1 Attestations exigées dans les Instructions uniformisées supplémentaires 2003-1

Les soumissionnaire doivent fournir les attestations réglementaires exigées conformément aux Instructions uniformisées supplémentaires - Télécommunications. Seuls les tarifs auxquels le soumissionnaire sera lui-même assujéti lors de l'exécution des travaux doivent être présentés. Il incombe au soumissionnaire de gérer sa relation avec les sous-traitants qui seraient assujéti à des tarifs.

5.2 Attestation pour le Code de conduite

Les soumissionnaires sont tenus de fournir une liste complète de toutes les personnes qui sont actuellement administrateurs de leur entreprise. Si un soumissionnaire n'a pas fourni cette liste à la fin de l'évaluation des soumissions, l'autorité contractante l'informerá du délai dans lequel l'information doit être fournie. Les soumissionnaires doivent fournir la liste des administrateurs avant l'attribution du contrat. S'ils n'ont pas fourni cette liste dans le délai prescrit, leur soumission sera déclarée irrecevable.

L'autorité contractante peut demander au soumissionnaire en tout temps durant la période du contrat subséquent, de remettre des formulaires de consentement dûment remplis et signés (formulaire Consentement à la vérification de l'existence d'un casier judiciaire – PWGSC-TPSGC 229) pour toute personne inscrite sur la liste susmentionnée, et ce, dans un délai prescrit. Si le soumissionnaire ne fournit pas le formulaire de consentement dans le délai précisé par l'autorité contractante, sa soumission sera déclarée irrecevable.

PART 6 EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Exigences relatives à la sécurité

- 6.1.1 À la date de clôture de la demande de soumissions, les conditions suivantes doivent être respectées :
- 6.1.1.1 le soumissionnaire doit détenir une attestation de vérification d'organisation désignée, comme indiqué à la Partie 7 – Clauses du contrat subséquent.
- 6.1.2 Pour obtenir d'autres renseignements sur les exigences de sécurité, on invite les soumissionnaires à consulter le document « Exigences de sécurité dans les demandes de soumissions de TPSGC – Instructions pour les soumissionnaires » sur le site Web Documents uniformisés d'approvisionnement ministériels (<http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-fra.html>).
- 6.1.3 Si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la sécurité.

6.2 Capacité financière

- 6.2.1 La clause A9033T (2012-07-16), Capacité financière, du Guide des clauses et conditions uniformisées d'achat (CCUA) s'applique. Cependant, le paragraphe 3 est supprimé et est remplacé par : « Si le soumissionnaire est une filiale d'une autre entreprise, chaque société mère, y compris la société mère ultime, devra fournir l'information financière demandée en 1(a) à (f). L'information financière fournie par une société mère ne dégage pas pour autant le soumissionnaire de l'obligation de présenter ses propres renseignements financiers; toutefois, si le soumissionnaire est une filiale d'une autre entreprise et que, dans le cours normal des affaires, les renseignements financiers de la filiale ne sont pas générés de façon distincte, les renseignements financiers de la société mère doivent être fournis. Si le Canada juge que le soumissionnaire ne possède pas la capacité financière nécessaire, mais que la société mère la possède, ou si le Canada ne peut évaluer la capacité financière du soumissionnaire puisqu'elle fait partie intégrante de celle de la société mère, le Canada peut, à sa seule discrétion, attribuer le marché au soumissionnaire sous réserve qu'au moins une des sociétés mères fournisse une garantie au Canada ».
- 6.2.2 Dans le cas d'une coentreprise, toutes les entreprises membres doivent satisfaire aux exigences financières.

PART 7 CLAUSES DU CONTRAT SUBSÉQUENT

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

7.1 Exigence

7.1.1 _____ (« **l'entrepreneur** ») consent à fournir au client les services décrits dans le contrat ainsi que dans l'Énoncé des travaux, conformément au présent contrat et aux prix énoncés dans ce dernier. Cela comprend :

- 7.1.1.1 la prestation de services d'interconnexion Internet (SII) sur demande;
- 7.1.1.2 la prestation d'un service de protection contre les attaques par DDOS, sur demande;
- 7.1.1.3 le déplacement de circuits, sur demande;
- 7.1.1.4 tout produit livrable requis conformément au contrat.

Les services ci-dessus seront fournis dans la région de la capitale nationale (RCN) et dans la région de Toronto (TOR), au Canada, à l'exclusion de tout lieu se trouvant dans des zones visées par les Ententes sur les revendications territoriales globales.

7.1.2 **Client** : Dans le cadre du contrat, le « **client** » est Services partagés Canada (SPC), une organisation dont le mandat est de fournir des services partagés. SPC se servira de ce marché pour fournir des services partagés à ses clients, soit lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant le marché, et les autres organisations qui choisissent de recourir à ses services, de temps en temps, à tout moment pendant le marché. SPC peut décider d'utiliser ce marché pour une partie ou l'ensemble de ses clients et peut avoir recours à d'autres moyens pour fournir les mêmes services ou des services semblables.

7.1.3 **Réorganisation du client** : La redésignation, la restructuration, le réaménagement ou le remaniement du client n'aura aucune incidence sur l'obligation de l'entrepreneur en ce qui a trait à l'exécution des travaux (et ne donnera pas lieu non plus au paiement d'honoraires supplémentaires). La restructuration, le réaménagement et le remaniement du client s'entendent également de sa privatisation, de sa fusion avec une autre entité et de sa dissolution, lorsque cette dissolution est suivie de la création d'une ou de plusieurs autres entités dont la mission est similaire à celle du client d'origine. Peu importe le type de réorganisation, le Canada peut désigner un autre ministère ou un autre organisme gouvernemental comme autorité contractante ou responsable technique, conformément aux nouveaux rôles et aux nouvelles responsabilités découlant de la réorganisation.

7.1.4 **Définition des termes** : Les termes et expressions définis dans les conditions générales ou les conditions générales supplémentaires et qui sont utilisés dans ce contrat ont le sens qui leur a été attribué dans ces conditions générales ou dans ces conditions générales supplémentaires. De plus, les termes et expressions ci-dessous ont les définitions suivantes :

7.1.4.1 « Jours ouvrables » désigne les jours du lundi au vendredi, à l'exception des jours fériés observés ci-dessous par le Canada :

- 7.1.4.1.1 Jour de l'An
- 7.1.4.1.2 Vendredi saint et lundi de Pâques
- 7.1.4.1.3 Fête de la Reine
- 7.1.4.1.4 Fête nationale du Québec (24 juin)
- 7.1.4.1.5 Fête du Canada
- 7.1.4.1.6 1^{er} lundi d'août
- 7.1.4.1.7 Fête du Travail
- 7.1.4.1.8 Action de grâce
- 7.1.4.1.9 Jour du Souvenir

7.1.4.1.10 Noël

7.1.4.1.11 Lendemain de Noël

7.2 Commandes de services

- 7.2.1 Les travaux devant être exécutés conformément aux dispositions du contrat seront commandés par le Canada au moyen d'une commande de services transmise à l'entrepreneur.
- 7.2.2 Les services décrits dans la commande doivent respecter la portée du marché. L'entrepreneur ne doit pas commencer à fournir les services tant qu'il n'a pas reçu de commande de services autorisée. Par conséquent, il accepte que toute tâche effectuée avant la réception de la commande de services soit effectuée à ses propres risques.
- 7.2.3 Lorsque l'entrepreneur reçoit une commande de services de l'autorité contractante, il accepte de fournir les services commandés, conformément aux conditions et aux prix ou tarifs énoncés dans le contrat. Sans considération pour la date de passation de la commande, toutes les commandes de services se terminent automatiquement au plus tard à la date de fin du marché; le Canada n'est donc pas tenu d'annuler les commandes à ce moment.
- 7.2.4 L'entrepreneur ne doit pas facturer au Canada plus que le coût total établi dans la commande de services, à moins que le Canada ait fait une modification de commande de services autorisant le coût accru. Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements, modifications ou interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.
- 7.2.5 L'entrepreneur doit, dans les 120 jours ouvrables du gouvernement fédéral suivant la date d'attribution du contrat, mettre au point une solution et un plan de mise en œuvre, en concertation avec le Canada, pour l'optimisation du transfert électronique des commandes de services à l'aide d'un outil électronique d'échange d'information approuvé, de l'acceptation d'une commande de services et de l'avis d'achèvement de la commande de services, de concert avec le Canada.
- 7.2.6 L'entrepreneur convient que les commandes de services peuvent être soumises par le Canada pour la fourniture de services 7 jours par semaine, 24 heures par jour, 365 jours par an (7x24x365) au moyen de l'outil électronique d'échange d'information approuvé.
- 7.2.7 Une fois que l'outil électronique d'échange d'information est accepté par le Canada, l'entrepreneur doit s'assurer que les commandes de services et toute modification à une commande de services reçue du Canada sont accessibles à l'aide de cet outil électronique.
- 7.2.8 Une commande de services doit, au minimum, comprendre les renseignements suivants :
- 7.2.8.1 le numéro de commande;
 - 7.2.8.2 la période à laquelle s'applique la commande;
 - 7.2.8.3 le numéro du contrat;
 - 7.2.8.4 la description des travaux commandés;
 - 7.2.8.5 le ou les emplacements précis des tâches et de la livraison, ainsi que les points de prestation de services (PPS);
 - 7.2.8.6 le coût total estimé des services fondé sur les tarifs et les prix énoncés dans le contrat s'appliquant à la durée de la commande de services;
 - 7.2.8.7 la base et la méthode de paiement s'appliquant aux services commandés.

7.3 Processus de commande de services

- 7.3.1 Le Canada transmettra une commande de services à l'entrepreneur pour les travaux qui doivent être fournis conformément au contrat, laquelle commande comprendra une date de début de prestation des services.
- 7.3.2 L'entrepreneur doit fournir une acceptation de la commande de services, par courriel ou au moyen d'une méthode de communication approuvée, à l'intérieur d'un (1) jour ouvrable du gouvernement

- fédéral (JOGF), confirmant la réception de la commande de services, et devra mettre à jour l'état de la commande de services dans l'outil électronique d'échange d'information pour indiquer que la commande a bien été reçue.
- 7.3.3 Dans les 2 JOGF, l'entrepreneur doit fournir au Canada une date de prestation de service promise (DPSP), qui sera assujettie à l'approbation écrite du Canada. La DPSP est la date à laquelle l'entrepreneur est tenu d'achever les travaux demandés dans la commande de services.
- 7.3.4 Si l'entrepreneur ne peut fournir le service demandé d'ici la DPSP, il est tenu d'aviser par écrit le Canada, le plus tôt possible avant cette date, en précisant la raison du retard ainsi qu'une DPSP révisée. Cette date révisée doit recevoir l'approbation écrite du Canada. Si le Canada n'approuve pas la date révisée, la DPSP initiale ne doit pas être modifiée.
- 7.3.5 Une fois que le Canada a approuvé la DPSP, les travaux sont assujettis au délai de prestation des services (DPS) pour cette commande de services, comme l'indique le tableau 4 ci-dessous.
- 7.3.6 Le délai de prestation des services est la période allouée à l'entrepreneur pour mettre en œuvre une commande de services. Le point de départ du DPS est la DPSP approuvée par le Canada. Le délai de prestation des services se termine à la DPSP. L'entrepreneur doit achever la prestation des services conformément au tableau 4 ci-dessous.
- 7.3.7 L'entrepreneur doit informer le Canada du succès des essais d'acceptation standard qu'il a réalisés, en lui envoyant par courriel un avis d'achèvement de la commande de services (AACS), à l'intérieur d'un (1) JOGF, après la fin de l'essai.
- 7.3.8 Dans cet avis d'achèvement de la commande de services, l'entrepreneur déclare officiellement que l'essai du nouveau service est terminé et que celui-ci est prêt à être utilisé.
- 7.3.9 L'AACS doit également comprendre la date d'achèvement des essais de l'entrepreneur et leurs résultats.
- 7.3.10 Les délais de prestation des services (DPS) figurent au tableau 4 – Exigences relatives aux délais de prestation des services.
- 7.3.11 Suivant la réception de l'AACS, le Canada a le droit d'effectuer ses propres essais d'acceptation dans les dix (10) JOGF.
- 7.3.12 Si le Canada effectue son propre essai d'acceptation dans les dix (10) JOGF suivant la date de l'AACS, et soumet un dossier d'incident au cours de cette période, l'exécution de la commande de services est considérée incomplète, et l'entrepreneur ne peut pas facturer le service.
- 7.3.13 L'entrepreneur doit aviser immédiatement le Canada par courriel de tout dossier d'incident soumis durant la période d'essai.
- 7.3.14 Lorsqu'une anomalie, détectée pendant les essais d'acceptation menés par le Canada, est corrigée par l'entrepreneur, le Canada dispose de dix (10) JOGF supplémentaires pour réaliser d'autres essais d'acceptation. Toute autre anomalie liée à la mise en œuvre du service signalée durant cette période relance la période d'essais d'acceptation de dix (10) JOGF, afin de permettre au Canada de mener d'autres essais d'acceptation.
- 7.3.15 La date de début de facturation pour les services qui satisfont aux essais d'acceptation du Canada est rétroactive à la date à laquelle le dernier dossier d'incident est fermé. Dans l'éventualité où l'anomalie signalée par le Canada ne serait pas attribuable à une faute de l'entrepreneur, la facturation commencerait à la plus tardive des dates suivantes : la date de réception de l'AACS ou la DPSP.
- 7.3.16 Si aucun dossier d'incident n'est soumis dans les dix (10) JOGF suivant la réception de l'AACS, la facturation commence de façon rétroactive à la plus tardive des dates suivantes : la DPSP ou la date de fin de l'essai d'acceptation de l'entrepreneur qui figure dans l'AACS.
- 7.3.17 Lorsque l'entrepreneur doit accéder aux locaux du gouvernement du Canada pour répondre à une commande de services, il doit en aviser le Canada au moins 48 heures à l'avance.
- 7.3.18 L'entrepreneur doit transmettre au Canada le numéro de circuit et l'information de configuration cinq (5) JOGF avant la DPSP.

Commande de services (Niveau de service-Délai de traitement des commandes de services)	DPS
Frais ponctuels (modifiant) : <ul style="list-style-type: none"> • pour modifier le débit de l'accès promis à 10 Gbps • Frais ponctuels pour modifier la capacité de la bande passante pour un déni de service distribué (DDOS) • Frais ponctuels par flux d'attaque supplémentaire pour la protection contre les attaques par DDOS 	5 JOGF
Frais ponctuels (déplacement) lorsque des installations existent : <ul style="list-style-type: none"> • en vue du déplacement de circuits, sur demande; ajout ou déplacement d'un circuit à un nouvel endroit où l'entrepreneur possède des installations de service et où le type d'accès commandé est disponible.	20 JOGF
Frais ponctuels (déplacement) lorsque des installations n'existent pas : <ul style="list-style-type: none"> • en vue du déplacement de circuits, sur demande; ajout ou déplacement d'un circuit à un nouvel endroit où l'entrepreneur ne possède pas d'installations de service, mais où il peut les construire et les livrer.	60 JOGF

Tableau 4 - Exigences relatives aux délais de prestation des services (DPS)

7.4 Modification à la commande de services

7.4.1 Une modification à la commande de services est une modification apportée à une commande de services, approuvée par l'autorité contractante et transmise à l'entrepreneur.

7.4.2 Modification à la commande de services

7.4.2.1 Le Canada peut, pour n'importe quelle raison, réduire ou augmenter les services d'une commande de services en publiant une modification à la commande de services. Si la modification réduit les services, la réduction entre en vigueur sept (7) jours civils après la publication de la modification. Le Canada paiera l'entrepreneur pour les services prévus dans la modification de commande de services, conformément aux dispositions de la base et de la méthode de paiement du contrat.

7.4.2.2 Si le Canada doit apporter une modification, une modification à la commande de services sera émise et envoyée à l'entrepreneur. La décision d'émettre ou non une modification à la commande de services relève exclusivement du Canada.

7.5 Garantie des travaux minimaux

7.5.1 Dans la présente clause, « **valeur minimale des travaux** » signifie 75 000,00 \$.

- 7.5.2 L'entrepreneur doit exécuter les travaux décrits dans le contrat à la demande du Canada pendant la durée du contrat. L'obligation du Canada, conformément au contrat, consiste à demander des travaux jusqu'à concurrence de la valeur minimale des travaux ou, au choix du Canada, à payer l'entrepreneur à la fin du contrat selon le paragraphe (7.5.3). En contrepartie, l'entrepreneur convient de se tenir prêt, pendant toute la durée du contrat, à exécuter les travaux décrits dans le contrat.
- 7.5.3 Si le Canada ne demande pas de travaux pour un montant correspondant à la garantie minimale des travaux pendant la période du contrat, le Canada paiera à l'entrepreneur la différence entre la garantie minimale des travaux et le coût des travaux achevés.
- 7.5.4 Le Canada n'aura aucune obligation envers l'entrepreneur en vertu de la présente clause s'il résilie le contrat en totalité ou en partie pour inexécution.

7.6 Clauses et conditions uniformisées

Toutes les clauses et conditions indiquées dans le contrat par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (<http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-fra.jsp>) publié par TPSGC. Toutes les références au ministre des Travaux publics et des Services gouvernementaux contenues dans les conditions générales et les conditions générales supplémentaires seront interprétées comme des références au ministre de qui relève la responsabilité de Services partagés Canada, et toutes les références à Travaux publics et Services gouvernementaux Canada seront interprétées comme des références à Services partagés Canada.

7.6.1 Conditions générales

- 7.6.1.1 2035 (2012-07-16), Conditions générales - besoins plus complexes de services, s'appliquent au marché et en font partie intégrante. Ces conditions générales sont modifiées comme suit :

La section 2 des Conditions générales est modifiée ainsi : supprimer « conformément à la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*, L.C. 1996, ch. 16 ».

- 7.6.1.2 Le texte du paragraphe 04 de la section 41 – Code de conduite et attestations, du document 2035 (2013-03-21), Conditions générales - besoins plus complexes de services, susmentionné est remplacé par ce qui suit :

4. Pendant toute la durée du contrat, l'entrepreneur doit diligemment tenir à jour la liste des administrateurs de l'entrepreneur et envoyer un avis écrit à l'autorité contractante chaque fois qu'un changement y est apporté. À la demande du Canada, l'entrepreneur doit aussi fournir les formulaires de consentement correspondants.

7.6.2 Conditions générales supplémentaires

Les conditions générales supplémentaires suivantes :

- 7.6.2.1 4005 (2012-07-16), Conditions générales supplémentaires – services et produits de télécommunication;

s'appliquent au contrat et en font partie intégrante.

7.7 Exigences relatives à la sécurité

- 7.7.1 L'entrepreneur doit, en tout temps durant l'exécution du contrat, de l'offre à commandes ou de l'arrangement en matière d'arrangement, maintenir une vérification d'organisation désignée (VOD) valide, comportant un système pour la sécurité des technologies de l'information, émise par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur et/ou son personnel, doivent TOUS maintenir une cote de fiabilité valide délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur doit maintenir une autorisation de détenir des renseignements (ADR) au niveau « protégé A » délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.

L'entrepreneur et/ou son personnel NE DOIVENT PAS emporter hors des établissements de travail visés des renseignements ou des biens CLASSIFIÉS et PROTÉGÉS B et C.

L'entrepreneur et/ou son personnel NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données CLASSIFIÉS et PROTÉGÉS B et C.

Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de Services partagés Canada.

L'entrepreneur et son personnel doivent se conformer aux dispositions des textes suivants :

- a) Justice Canada – *Loi sur la protection de l'information* (dernière version);
- b) Manuel de la sécurité industrielle (dernière édition).

7.7.2 Mesures de sécurité générales entourant la transmission de données sensibles

7.7.2.1 Les services de télécommunications fournis conformément au contrat seront utilisés pour la transmission des données du gouvernement du Canada de divers genres, y compris les communications sécurisées (à divers niveaux de classification de sécurité), les communications privilégiées (comme les documents confidentiels du Cabinet et les communications assujetties au secret professionnel) et les communications autrement sensibles (y compris les transmissions contenant des renseignements personnels des Canadiens et des renseignements exclusifs ou confidentiels de tierces parties, comme les fournisseurs).

7.7.2.2 L'entrepreneur reconnaît que le Canada a besoin des services de télécommunications fournis conformément au contrat, et il garantit qu'il le fournira toujours conformément au contrat. Il garantit aussi que ce service s'accompagnera de mesures de sécurité robustes et exhaustives qui évolueront en même temps que les menaces de sécurité et les technologies, ce qui signifie que les mesures de sécurité utilisées doivent être mises à jour pendant toute la durée du contrat afin de réaliser le niveau le plus élevé possible d'intégrité, de disponibilité et de confidentialité des données.

7.7.2.3 L'entrepreneur doit mettre en œuvre toutes les mesures de sécurité ou de protection raisonnables demandées par le Canada de temps à autre, dans un délai raisonnable convenu avec le Canada. Les parties conviennent de déterminer le caractère raisonnable selon la gravité de la menace à l'intégrité, à la disponibilité et à la confidentialité des données et des communications du Canada.

7.7.3 Attestation de sécurité

7.7.3.1 L'entrepreneur reconnaît que le Canada peut préciser qu'un équipement ou un réseau est sensible au plan de la sécurité et imposer une classification de sécurité dans lequel cas seuls les employés et les entrepreneurs ayant une cote de sécurité peuvent travailler au système. Les personnes qui ne possèdent pas de cote de sécurité peuvent seulement aider à travailler au système, mais ne sont pas autorisées à contrôler ou à charger le logiciel.

7.7.3.2 L'accès à distance à certains systèmes peut être autorisé, mais toutes les frappes au clavier et tous les logiciels téléchargés doivent être copiés et conservés à titre de preuves judiciaires, le cas échéant.

7.7.3.3 Dès leur arrivée dans les installations du Canada, tous les employés de l'entrepreneur et du sous-traitant approuvés au préalable par l'autorité contractante doivent être en mesure de fournir une preuve d'emploi (comme un insigne émis par l'entrepreneur ou par le sous-traitant approuvé), et le statut de leur attestation de sécurité doit être validé par une source sûre.

7.7.3.4 Des personnes qui, même si elles n'ont pas accès à l'information ou des biens CLASSIFIÉS, peuvent occuper des postes qui sont jugés essentiels à l'intérêt national. Il s'agit entre autres du personnel qui a un accès privilégié offrant la possibilité de perturber ou d'endommager de façon

importante des systèmes essentiels. Ces personnes doivent faire l'objet d'une enquête de sécurité et obtenir une habilitation de sécurité du niveau SECRET au moins. Par exemple, le personnel technique ou opérationnel, y compris les administrateurs ou les gestionnaires de réseaux ou de systèmes, qui contrôle directement les fonctionnalités les plus sensibles et essentielles comme la surveillance, la détection, la sauvegarde et la récupération de l'information, la mise à l'essai et l'installation de correctifs de sécurité, les changements de configuration au matériel et au logiciel de sécurité, la réaction aux incidents de sécurité, etc. NOTA : Les contrôles d'accès additionnels sont aussi requis comme la séparation des tâches, afin d'assurer que personne n'a un accès trop grand aux fonctionnalités les plus sensibles. Des dossiers de vérification de sécurité doivent être disponibles afin d'assurer qu'un tel accès peut être suivi par vérification jusqu'à une personne en particulier.

7.7.3.5 L'entrepreneur reconnaît que le Canada peut, en tout temps, refuser à une personne l'accès à ses locaux. Si cette personne répond aux exigences relatives à l'attestation de sécurité pour le type de travail accompli, mais que le Canada refuse de lui fournir l'accès nécessaire, le délai d'exécution de son travail indiqué sur le contrat ne commencera pas avant que le Canada informe l'entrepreneur qu'un accès a été accordé à cette personne. Le Canada peut informer l'entrepreneur de sa raison pour refuser l'accès, mais peut aussi ne pas le faire s'il a déterminé, à sa discrétion, qu'il y avait des raisons de sécurité pour ne pas divulguer la raison.

7.7.3.6 L'entrepreneur doit obtenir l'attestation de sécurité requise pour tout son personnel avant l'attribution du contrat. Après l'attribution du contrat, il appartient entièrement à l'entrepreneur de faire en sorte d'avoir suffisamment d'employés autorisés au niveau indiqué dans le contrat pour exécuter les travaux.

7.7.3.7 L'entrepreneur reconnaît que le Canada peut, à tout moment, révoquer l'attestation de sécurité d'un employé.

7.7.4 **Sous-traitance**

7.7.4.1 Sous-traitance : Malgré les conditions générales, aucune partie des travaux ne peut être sous-traitée (même à une société affiliée de l'entrepreneur) sans le consentement écrit préalable de l'autorité contractante. Pour obtenir le consentement écrit de l'autorité contractante, l'entrepreneur doit fournir les renseignements suivants :

7.7.4.1.1 Le nom du sous-traitant;

7.7.4.1.2 La partie des travaux qui sera effectuée par le sous-traitant;

7.7.4.1.3 La vérification d'organisation désignée ou l'attestation de sécurité d'installation (ASI) du sous-traitant, selon les besoins des travaux;

7.7.4.1.4 Sur demande, l'attestation de sécurité des employés du sous-traitant qui devront avoir accès aux installations du Canada;

7.7.4.1.5 La Liste de vérification des exigences génériques relatives à la sécurité (LVERS) secondaire remplie et signée par l'agent de sécurité d'entreprise de l'entrepreneur, en vue d'être remplie par la Direction de la sécurité industrielle canadienne (DSIC);

7.7.4.1.6 Tout autre renseignement exigé par l'autorité contractante.

7.7.5 **Schéma du réseau**

7.7.5.1 Dans les 30 jours civils suivant l'attribution du contrat, l'entrepreneur doit fournir au responsable technique une ébauche du schéma du réseau comprenant, au minimum, les éléments suivants :

7.7.5.1.1 la topologie du réseau physique et logique illustrant les nœuds et les connexions entre les nœuds du réseau;

7.7.5.1.2 des détails sur les nœuds du réseau, les protocoles, les largeurs de bande, etc.

7.7.5.2 L'entrepreneur doit fournir un schéma du réseau mis à jour pour le Canada dans les 3 JOGF après tout changement qui doit refléter toutes les modifications apportées au réseau. Même quand il n'y a aucun changement, l'entrepreneur est tenu d'émettre de nouveau le schéma du

réseau avec les nouvelles dates au moins pour chaque trimestre, dans les 2 semaines suivant la fin de chaque période de rapport.

7.7.5.3 L'entrepreneur reconnaît que le schéma du réseau ne lui appartient pas.

7.7.6 **Emplacement des bases de données, acheminement du trafic dans le réseau et données**

7.7.6.1 L'entrepreneur doit s'assurer que toutes les bases de données contenant l'information relative aux travaux (y compris la facturation et/ou les données d'appel) ou que toutes les données sont situées au Canada.

7.7.6.2 L'entrepreneur doit s'assurer que toutes les bases de données comprenant des données relatives au présent et archivées sont isolées sur les plans physique et logique, en d'autres termes qu'elles n'ont aucune connexion directe ou indirecte de quelque type que ce soit avec d'autres bases de données.

7.7.6.3 L'entrepreneur doit s'assurer qu'il est possible d'accéder aux données concernant ce contrat et de les traiter uniquement au Canada ou dans une administration autre approuvée par l'autorité contractante conformément au paragraphe (7.6.8.1 ci-dessus).

7.7.6.4 L'entrepreneur doit s'assurer que le trafic sur le réseau national (c'est-à-dire le trafic partant d'une partie du Canada vers une destination située dans une autre partie du Canada) s'effectue exclusivement au Canada.

7.7.7 **Connectivité et contrôle d'accès au réseau**

7.7.7.1 En tout temps, l'entrepreneur doit protéger le réseau et toutes les bases de données, y compris les données du Canada ou les renseignements concernant le Canada, en prenant toutes les mesures raisonnablement nécessaires pour les sécuriser et protéger leur intégrité et leur confidentialité. Pour ce faire, l'entrepreneur doit, au minimum :

7.7.7.1.1 contrôler l'accès à toutes les bases de données dans lesquelles des données concernant ce contrat sont stockées de sorte que seules les personnes ayant l'attestation de sécurité requise en vertu du contrat et qui ont besoin d'accéder à l'information afin d'exécuter le contrat peuvent avoir accès à la base de données;

7.7.7.1.2 s'assurer que les mots de passe ou les autres contrôles d'accès ne sont fournis qu'aux personnes qui en ont besoin pour exécuter les travaux et qui possèdent l'attestation de sécurité délivrée par la DSIC au niveau requis conformément aux exigences contractuelles;

7.7.7.1.3 protéger toutes les bases de données ou tous les systèmes informatiques qui contiennent des données du Canada contre un accès externe par des méthodes couramment utilisées par des organismes publics et privés du Canada faisant preuve de prudence dans le but de protéger les renseignements très protégés et sensibles.

7.7.7.1.4 L'entrepreneur doit démontrer qu'il suit des pratiques judicieuses en matière de sécurité pour ce qui est de la conception et de la mise en œuvre, à l'aide d'un processus officiel de gestion des risques liés à la sécurité, tel que l'ITSG-33, « La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie » et, par conséquent, doit fournir une évaluation de sécurité et une preuve d'assurance pour valider que :

7.7.7.1.4.1 (1) les contrôles de sécurité appropriés sont sélectionnés pour répondre aux besoins opérationnels applicables liés à la sécurité, et que des pratiques exemplaires de sécurité sont conçues pour atténuer la vulnérabilité aux menaces;

7.7.7.1.4.2 (2) ces contrôles sont mis en œuvre efficacement dans un environnement opérationnel.

7.7.7.2 Le développement, la mise à l'essai en direct ou la gestion des réseaux doivent être isolés l'un de l'autre et des réseaux du Canada.

7.7.7.3 À moins que le responsable technique ne le demande, l'entrepreneur doit désactiver les ports d'écoute TCP/UDP pour tout l'équipement déployé dans le réseau du Canada ou dans l'infrastructure de réseau ou le réseau de base de l'entrepreneur qui est interconnecté au

réseau du Canada. Des méthodes de contrôle d'accès strictes doivent être en place pour tous les ports ouverts aux fins de gestion du réseau.

L'entrepreneur doit conserver un registre de vérification qui enregistre automatiquement toutes les tentatives d'accès au réseau du Canada, ainsi qu'à toutes les bases de données qui comprennent les données ou des renseignements sur le Canada conservés par l'entrepreneur (comme des renseignements sur la facturation et des renseignements détaillés sur les appels). Chaque action, transaction ou fonction opérationnelle exécutée sur le réseau, les systèmes ou les bases de données de l'entrepreneur liés au contrat doit pouvoir être rattachée à un utilisateur ou un compte individuel (en s'assurant que les identificateurs et les comptes des utilisateurs sont uniques et qu'ils ne peuvent pas être partagés ou transférés d'une personne à une autre).

7.7.8 Protocoles de gestion de réseau

- 7.7.8.1 L'entrepreneur doit s'assurer que l'équipement ou tous les composants qui font partie du système utilisé pour assurer la prestation des services de réseau peuvent être gérés au moyen de protocoles sécurisés.
- 7.7.8.2 Si l'entrepreneur utilise des serveurs de gestion qui ont un niveau de sécurité ou de chiffrement configurable, l'entrepreneur doit désactiver tous les niveaux autres que le niveau le plus élevé de sécurité et/ou de chiffrement.
- 7.7.8.3 L'entrepreneur évitera d'employer des protocoles selon lesquels les noms d'utilisateur et mots de passe sont transmis en clair dans le réseau.
- 7.7.8.4 L'entrepreneur ne doit pas utiliser de protocoles (et doit les désactiver) qui ne peuvent pas passer par des coupe-feu compatibles avec la session.
- 7.7.8.5 Le Canada ne considérera pas qu'un protocole autrement non sécurisé est sécurisé même s'il a fait l'objet de l'utilisation de techniques de tunnellation comme la redirection de port ou le protocole IpSec (IPSec).
- 7.7.8.6 L'entrepreneur doit mettre en œuvre les protocoles de chiffrement relevés par le Canada et désactiver tous les protocoles de chiffrement qui ne sont pas approuvés par celui-ci.

7.7.9 Évaluation et gestion de la vulnérabilité

- 7.7.9.1 L'entrepreneur doit fournir au responsable technique des renseignements opportuns sur les vulnérabilités (c.-à-d. les faiblesses ou les lacunes de conception cernées dans l'équipement fourni selon le contrat/tout élément du système utilisé pour fournir les services du réseau qui permettraient à une personne non autorisée de compromettre l'intégrité, la confidentialité, les contrôles d'accès, la disponibilité, la cohérence ou le mécanisme de vérification du système ou des données et applications qu'il héberge).
- 7.7.9.2 Lorsqu'une vulnérabilité est causée par l'équipement ou le code de logiciel fabriqué ou écrit par l'entrepreneur ou l'un de ses sous-traitants, ce dernier doit immédiatement corriger la vulnérabilité à ses propres frais.
- 7.7.9.3 Lorsqu'une vulnérabilité est causée par l'équipement ou par le code de logiciel fabriqué ou écrit par une tierce partie (autre qu'un sous-traitant), en plus d'aviser le responsable technique de la vulnérabilité dès qu'il en est mis au courant, l'entrepreneur doit mettre en œuvre les mises à niveau, les correctifs ou toute autre mesure corrective dans un délai acceptable pour le Canada, une fois qu'ils ont été mis à sa disposition par le fabricant ou l'éditeur de logiciel, aux frais de l'entrepreneur, à moins que le responsable technique ne fasse abstraction de cette exigence (en regard d'une mise à niveau, d'un programme ou d'une mesure corrective) par écrit.

7.7.10 Surveillance de sécurité et rapport d'incident

- 7.7.10.1 L'entrepreneur doit surveiller les activités anormales ou suspectes dans le réseau comme les heures de travail inusitées, des demandes de code ou de données inutiles, des mouvements de données anormales ou une utilisation excessive des systèmes ou des ressources.
- 7.7.10.2 L'entrepreneur doit signaler immédiatement au responsable technique et à la DSIC tout incident relatif à la sécurité du réseau du Canada, de sa propre infrastructure ou de son réseau de base ou des données du Canada, si cela a une incidence sur le Canada, y compris les

incidents décrits au paragraphe (7.6.12.1). Par exemple, tout accès ou toute tentative d'accès non autorisé doit être signalé immédiatement. Les virus, les programmes malveillants et l'installation non autorisée de code de logiciel doivent également être signalés sur-le-champ, peu importe leur emplacement.

7.7.10.3 L'entrepreneur convient de collaborer entièrement avec le Canada dans une enquête entourant tout incident de sécurité.

7.7.11 Vérification de sécurité

Le Canada peut à tout moment vérifier si l'entrepreneur respecte les exigences de sécurité contenues dans le contrat. À la demande de l'autorité contractante, l'entrepreneur doit donner au Canada (ou au représentant autorisé du Canada) l'accès complet à ses locaux, à son réseau et à toutes les bases de données contenant des données du Canada ou des données liées au contrat, à toute heure convenable. Si le Canada découvre une faille de sécurité durant la vérification, l'entrepreneur la corrigera immédiatement, à ses frais.

7.8 Sécurité de la chaîne d'approvisionnement

7.8.1 À tout moment durant la période du contrat, si l'entrepreneur propose d'introduire de nouveaux produits commerciaux, qui ne faisaient pas partie de la liste des produits de TI approuvés par le Canada, dans le réseau du Canada ou dans l'infrastructure de l'entrepreneur ou son réseau de base, ou dans ceux de la tierce partie, produits qui seront interconnectés avec le réseau du Canada, l'entrepreneur doit obtenir au préalable l'approbation écrite du responsable technique. Le Canada se réserve le droit de refuser de nouveaux produits commerciaux, de proposer de nouvelles mesures de protection, de valider de façon indépendante et d'approuver les produits commerciaux.

7.8.2 À tout moment, si le Canada avise l'entrepreneur qu'un fabricant ou un fabricant original de matériel (OEM) n'est plus considéré comme un fabricant de confiance ou un OEM (c.-à-d. un fabricant en qui on ne fait plus confiance), l'entrepreneur (et ses sous-traitants) doit immédiatement cesser de déployer l'équipement manufacturé par le fabricant ou l'OEM dans le réseau du Canada et dans toute infrastructure ou réseau de base de l'entrepreneur qui se raccordera au réseau du Canada. Pour ce qui est de l'équipement déjà déployé, l'entrepreneur doit identifier et/ou enlever l'équipement manufacturé par ce fabricant ou cet OEM qui serait dans le réseau du Canada et dans toute infrastructure ou réseau de base de l'entrepreneur qui se raccordera au réseau du Canada. Si le Canada demande que l'on apporte une modification conformément à cette section, l'entrepreneur a droit à un rajustement équitable.

7.8.3 Si l'entrepreneur est informé qu'un tiers (sauf un sous-traitant) déploie un équipement non éprouvé sur son réseau, il doit immédiatement en informer le responsable technique.

7.8.4 Changement de contrôle

Aux fins des Conditions générales 2035 (2012-03-02) - besoins plus complexes de services, le terme « cession » comprend, sans s'y limiter, les changements de contrôle dans les cas où l'entrepreneur est une société, qu'il s'agisse d'un changement direct ou indirect dans le contrôle effectif de cette société et que ce changement découle d'une vente, de charges, d'une cession des actions ou d'autres raisons.

7.9 Durée du contrat

7.9.1 **Durée du contrat :** La « durée du contrat » est la période pendant laquelle l'entrepreneur doit effectuer les travaux et englobe :

7.9.1.1 la « période initiale du contrat », qui commence à la date d'attribution du contrat et se termine trois (3) ans plus tard;

7.9.1.2 la période durant laquelle le contrat est prolongé, si le Canada décide de se prévaloir des options stipulées au contrat.

7.9.2 Option de prolongation du contrat :

7.9.2.1 L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus une période additionnelle de une (1) année, selon les mêmes conditions. L'entrepreneur

accepte, au cours de la période prolongée du marché, d'être payé conformément aux dispositions applicables définies dans la Base de paiement.

7.9.2.2 La période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines; Cette option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

7.10 Responsables

7.10.1 Autorité contractante

L'autorité contractante pour le marché est :

Nom : Mark Hall
Titre : Spécialiste de l'approvisionnement
Ministère : Services partagés Canada
Direction de l'approvisionnement en services partagés de technologie de l'information
Adresse : 11, rue Laurier, Gatineau (Québec) K1A 0S5
Téléphone : 819-956-0251
Télécopieur : 819-956-9191
Courriel :: mark.hall@ssc.gc.ca

L'autorité contractante est responsable de la gestion du contrat et doit autoriser toute modification par écrit. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou de travaux qui n'y sont pas prévus par suite de demandes ou d'instructions verbales ou écrites de toute personne autre que l'autorité contractante.

7.10.2 Responsable technique

Le responsable technique pour le marché est :

< À insérer au moment de l'attribution du contrat >

L'autorité fonctionnelle est responsable de toutes les questions qui concernent le contenu technique des travaux en vertu du contrat. On peut discuter des questions techniques avec le responsable technique; cependant, celui-ci ne peut pas autoriser les changements à apporter à la portée des travaux. Ces changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

7.10.3 Représentant de l'entrepreneur

< À insérer au moment de l'attribution du contrat >

7.11 Paiement

7.11.1 Base de paiement

- 7.11.1.1 **Services d'interconnexion Internet (SII)** : Pour la prestation de services d'interconnexion Internet, conformément au contrat, le Canada versera à l'entrepreneur un montant mensuel récurrent, comme établi à l'annexe B, TPS, TVQ ou TVH en sus.
- 7.11.1.2 **Modification du taux promis pour les SII** : S'il souhaite modifier le taux promis de l'accès à 10 gigabits par seconde, conformément au contrat, le Canada paiera à l'entrepreneur un prix d'installation non récurrent, comme établi à l'annexe B, TPS, TVQ ou TVH en sus.
- 7.11.1.3 **Protection contre les attaques par DDOS** : Pour la prestation d'un service de protection contre les attaques par DDOS jusqu'à concurrence de cinq (5) flux d'attaque, conformément au contrat, le Canada versera à l'entrepreneur un montant mensuel récurrent, comme établi à l'annexe B, TPS, TVQ ou TVH en sus.
- 7.11.1.4 **Flux d'attaque par DDOS supplémentaires** : Pour la prestation d'un service de protection contre d'autres flux d'attaque, soit plus que les cinq (5) flux continus mentionnés au paragraphe 7.10.1.3 ci-dessus, conformément au contrat, le Canada versera à l'entrepreneur,

pour chaque flux additionnel, un montant mensuel récurrent, comme établi à l'annexe B, TPS, TVQ ou TVH en sus.

7.11.1.5 **Frais ponctuels d'installation non récurrents (FINR)** : Les frais ponctuels pour le déplacement de SII existants ou l'installation de SII supplémentaires sont seulement permis si au moins un des critères ci-dessous s'applique :

- i) des installations d'accès (y compris des conduits entre la limite de propriété et le bâtiment) sont requises, car il n'en existe pas ou celles qui existent sont utilisées à plein rendement ou sont endommagées et non réparables;
- iv) les SII existants doivent être déplacés à l'endroit où l'équipement terminal actuel sera déplacé et seront réutilisés au nouveau site.

7.11.1.6 **Taxes** : Le Canada versera la TPS, la TVQ ou la TVH à l'entrepreneur, selon le cas.

7.11.1.7 Calcul au prorata pour les mois partiels : Lorsque les services sont acceptés ou résiliés à une date autre que le premier ou dernier jour du mois, l'entrepreneur doit répartir le tarif mensuel applicable en fonction du nombre de jours de service dans un mois de 30 jours.

7.11.1.8 Lorsque le contrat comporte des travaux pour lesquels il n'existe pas de postes distincts dans la base de paiement ou dans l'annexe B, Prix des SII, les prix pour ces travaux sont inclus dans les tarifs/prix pour les services, tels qu'ils sont détaillés à l'annexe B, Prix des SII.

7.11.1.9 Transition des services vers l'entrepreneur - phase de mise en œuvre

7.11.1.9.1 Le montant payable à l'entrepreneur pour les services inclus dans toute commande de services sera égal à zéro au début de la phase de mise en œuvre du service et augmentera progressivement avec chaque période de facturation, au fur et à mesure que l'entrepreneur s'emploiera à rendre les services opérationnels et que ces services seront acceptés par le Canada.

7.11.1.10 Transition des services à la fin de la période du contrat

7.11.1.10.1 Le montant payable à l'entrepreneur pour les services inclus toute commande de services diminuera en conformité avec les services résiliés au cours de chaque période de facturation. Il ne doit y avoir aucun coût pour le Canada ni frais de tout type ou pour toute autre raison liés au temps de l'entrepreneur et aux efforts de suppression progressive des services au cours de la phase de résiliation du contrat.

7.11.1.11 **Attribution concurrentielle** : L'entrepreneur reconnaît que ce marché a été attribué selon un régime concurrentiel. Aucuns frais supplémentaires ne seront payés à l'entrepreneur pour compenser les erreurs, les omissions, les méprises ou les sous-estimations de l'entrepreneur dans le cadre du dépôt d'une soumission pour l'obtention du contrat.

7.11.1.12 **Objet des estimations** : Toutes les estimations contenues dans ce contrat le sont uniquement pour répondre aux besoins administratifs du Canada et ne constituent pas des engagements de sa part pour ce qui est de l'acquisition de biens ou de services selon les quantités indiquées. Les engagements relatifs à l'acquisition d'une quantité ou d'une valeur précise de biens ou de services sont décrits ailleurs dans le contrat.

7.11.2 Limitation des dépenses

7.11.2.1 L'entrepreneur sera remboursé pour les coûts qu'il a engagés raisonnablement et convenablement dans l'exécution des travaux décrits dans la commande de services (CS) approuvée, comme ils ont été déterminés conformément à la base de paiement détaillée ci-dessous, jusqu'à la limitation des dépenses indiquée dans la commande de services (CS) autorisée.

7.11.2.2 La responsabilité du Canada envers l'entrepreneur dans le cadre de la CS ne doit pas dépasser la limitation des dépenses précisée dans la CS autorisée. Les droits de douane sont exclus et la taxe sur les produits et services, la taxe de vente du Québec ou la taxe de vente harmonisée est en sus, s'il y a lieu.

7.11.2.3 Aucune augmentation de la responsabilité du Canada ou du prix des travaux précisé dans la CS autorisée découlant de tout changement à la conception, ou de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements à la conception, aux modifications ou aux interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés aux travaux.

7.11.3 Méthode de paiement pour les commandes de services - Paiement mensuel

7.11.3.1 H1008C (2008-05-12), Paiements multiples

7.11.4 Méthode de paiement pour les commandes de services - Paiement unique

7.11.4.1 H1000C (2008-05-12) Paiement unique

7.11.5 Crédits de paiement

S'il ne satisfait pas aux exigences en matière de niveaux de service, de prestation de services et de délai de réponse énoncées à l'annexe A de l'énoncé des travaux ou ailleurs dans le contrat, l'entrepreneur doit accorder des crédits au Canada. Il doit inclure les crédits de service dans la facture mensuelle suivant le mois pendant lequel ils ont été accordés. Les crédits applicables doivent être calculés comme un pourcentage de la facture mensuelle totale pour les services en question, selon la méthode ci-dessous.

7.11.5.1 **Incapacité de fournir le niveau de disponibilité demandé des services Internet et de protection contre les attaques par DDOS** : Si l'entrepreneur dépasse le délai maximal de rétablissement du service pour les services Internet et de protection contre les attaques par DDOS décrits à l'annexe A de l'énoncé des travaux pendant un mois donné, il doit accorder des crédits au Canada selon les indications du tableau 1 ci-dessous.

Délai de rétablissement mensuel total	Crédit de service
Délai <= 40 minutes	0 %
40 minutes < délai <= 3 heures	10 %
3 heures < délai <= 4,5 heures	25 %
Délai > 4,5 heures	50 %

Tableau 1 : Crédits de service

7.11.5.2 **Incapacité de fournir le niveau de service minimum pour la transmission de données, le délai de livraison de paquets et la perte de paquets** : S'il ne respecte pas les niveaux de service minimaux décrits à l'annexe A de l'énoncé des travaux pendant un mois donné, l'entrepreneur doit accorder des crédits au Canada selon les indications du tableau 2.

Total mensuel d'heures de services pendant lesquelles le niveau de service minimum n'est pas fourni	Crédit de service
de 2 à 3 heures	10 %
de 4 à 6 heures	25 %
> 6 heures	50 %

Tableau 2 : Crédits de service

7.11.5.3 Incapacité de respecter les délais de traitement des commandes de services :

- 7.11.5.3.1 L'entrepreneur doit accorder un crédit de service au Canada selon un pourcentage des frais de service mensuels totaux de la commande de services en question pour chaque jour ouvrable où il dépasse la date de prestation de service promise (DPSP), comme l'indique le tableau 3.

$$\text{Crédit de service} = (\text{coût mensuel total du service en question}) \times (\text{pourcentage du crédit de service}) \times (\text{nombre de jours ouvrables suivant la DPSP})$$

- 7.11.5.3.2 Lorsqu'il ne respecte pas la DPSP, l'entrepreneur doit calculer le crédit de service qui s'applique pour une nouvelle commande de services en fonction du montant mensuel total de ce nouveau service pour le premier mois complet suivant l'exécution de la commande de services.

Commande de services (Niveau de service-Délai de traitement des commandes de services)	Crédit de service (% par jour ouvrable où cela dépasse la DPSP pour le service en question)
Frais ponctuels (modifiant) : <ul style="list-style-type: none"> pour modifier le débit de l'accès promis à 10 Gbps Frais ponctuels pour modifier la capacité de la bande passante pour un déni de service distribué (DDOS) Frais ponctuels par flux d'attaque supplémentaire pour la protection contre les attaques par DDOS 	10 %
Frais ponctuels (déplacement) lorsque des installations existent : <ul style="list-style-type: none"> en vue du déplacement de circuits, sur demande; ajout ou déplacement d'un circuit à un nouvel endroit où l'entrepreneur possède des installations de service et où le type d'accès commandé est disponible.	10 %
Frais ponctuels (déplacement) lorsque des installations n'existent pas : <ul style="list-style-type: none"> en vue du déplacement de circuits, sur demande; ajout ou déplacement d'un circuit à un nouvel endroit où l'entrepreneur ne possède pas d'installations de service, mais où il peut les construire et les livrer.	10 %

Tableau 3 : Crédits de service pour les délais de prestation de services

- 7.11.5.4 **Mesures correctives** : Si, conformément à cet article, les crédits sont applicables durant deux (2) mois consécutifs ou durant trois (3) mois sur une période de douze (12) mois, l'entrepreneur doit présenter un plan d'action écrit décrivant les mesures qui seront prises pour éviter que le problème ne se produise de nouveau. L'entrepreneur aura cinq jours ouvrables pour présenter le plan d'action au Canada et à l'autorité contractante, et vingt jours ouvrables pour corriger la source du problème.

- 7.11.5.5 **Résiliation pour non-respect du niveau de disponibilité minimal** : En plus de tous ses autres droits dans le cadre du contrat, le Canada peut résilier le contrat pour manquement, conformément aux conditions générales, en donnant à l'entrepreneur un avis écrit de trois (3) mois lui faisant part de son intention, si l'une de ces conditions s'applique :
- 7.11.5.5.1 le montant total de crédits pour tout cycle mensuel de facturation atteint un niveau de 10 %; ou
- 7.11.5.5.2 les mesures correctives présentées par l'entrepreneur n'ont pas été prises.
- La résiliation du contrat entrera en vigueur à la fin de la période de trois (3) mois, sauf si l'entrepreneur répond au niveau de disponibilité minimal au cours de cette période.
- 7.11.5.6 **Crédits applicables pendant toute la durée du contrat** : Les parties conviennent que les crédits s'appliquent tout au long de la durée du contrat, y compris durant la mise en œuvre.
- 7.11.5.7 **Crédits représentant des dommages-intérêts** : Les parties conviennent que les crédits sont des dommages-intérêts et qu'ils représentent leur meilleure estimation préalable de la perte pour le Canada dans l'éventualité du manquement applicable. Les crédits ne visent pas à constituer une pénalité, et ne doivent pas être considérés comme constituant une pénalité.
- 7.11.5.8 **Droit du Canada d'obtenir le paiement** : Les parties conviennent que ces crédits représentent une dette déterminée. Le montant des crédits peut, en tout temps, être retenu, recouvré, déduit ou faire l'objet d'une compensation, par le Canada, sur toute somme due à l'entrepreneur par le Canada.
- 7.11.5.9 **Droits et recours du Canada non limités** : Les parties conviennent que rien dans le présent article ne limite les droits ni les recours dont le Canada peut se prévaloir conformément au contrat (y compris le droit de résilier le contrat pour manquement) ou de la loi en général.
- 7.11.5.10 **Droits de vérification** : Le calcul de l'entrepreneur relatif aux crédits conformément au contrat peut être vérifié par le service de vérification du gouvernement, à la discrétion de l'autorité contractante, avant que le paiement ne soit fait à l'entrepreneur ou après. L'entrepreneur doit coopérer entièrement avec le Canada au cours de la réalisation de toute vérification en permettant au Canada d'accéder à tous les documents et systèmes que le Canada juge nécessaires pour veiller à ce que tous les crédits aient été correctement imputés au Canada dans les factures de l'entrepreneur. Si une vérification démontre que des factures passées contiennent des erreurs de calcul des crédits, l'entrepreneur doit payer au Canada le montant, tel qu'il a été déterminé par la vérification, qui aurait dû être crédité au Canada, additionné des intérêts, à compter de la date à laquelle le Canada a versé le paiement excédentaire jusqu'à la date du remboursement (le taux d'intérêt correspond au taux officiel d'escompte par année de la Banque du Canada en vigueur à la date à laquelle le crédit était d'abord dû au Canada, plus 1,25 % par année). Si, à la suite de la réalisation d'une vérification, le Canada détermine que les documents ou les systèmes de l'entrepreneur servant à déterminer, à calculer ou à enregistrer les crédits ne sont pas adéquats, l'entrepreneur doit mettre en œuvre toutes les mesures supplémentaires exigées par l'autorité contractante.
- 7.11.6 **Aucune obligation de payer pour des travaux non effectués en raison de la fermeture des bureaux du gouvernement**
- 7.11.6.1 Dans le cas où l'entrepreneur, ses employés, ses sous-traitants ou ses agents offrent des services dans les locaux du gouvernement en vertu de ce contrat et que ces locaux sont inaccessibles en raison d'une évacuation ou de la fermeture des bureaux du gouvernement, et qu'aucun travail n'a pu être effectué pour cette raison, le Canada ne pourra être tenu responsable de payer l'entrepreneur pour les travaux qui auraient pu être effectués si les bureaux n'avaient pas été évacués ou fermés.
- 7.11.6.2 Dans le cas où l'entrepreneur, ses employés, ses sous-traitants ou ses agents ne peuvent pas, en raison d'une grève ou d'un lock-out, entrer dans les locaux durant une certaine période, et qu'aucun travail ne peut être effectué pour cette raison, le Canada ne pourra être tenu responsable de payer l'entrepreneur pour les travaux qui auraient pu être effectués si l'entrepreneur avait eu accès aux locaux.

7.12 Instructions relatives à la facturation

- 7.12.1 L'entrepreneur doit présenter ses factures conformément à l'information exigée dans les conditions générales.
- 7.12.2 La facture de l'entrepreneur doit inclure un article pour chaque sous-alinéa des clauses de la Base de paiement.
- 7.12.3 En présentant des factures, l'entrepreneur atteste que les produits et services ont été livrés et que tous les frais sont conformes aux dispositions de la base de paiement de ce marché, y compris tous frais pour des travaux effectués par des sous-traitants.
- 7.12.4 L'entrepreneur doit envoyer la version originale de chaque facture à l'adresse suivante :
- Services partagés Canada
Bureau des comptes fournisseurs de télécommunications
Place du Portage, Phase III, Section 5A2
11, rue Laurier
Gatineau (Québec) K1A 0S5
- 7.12.5 L'entrepreneur doit aussi soumettre à l'autorité contractante une copie électronique en format PDF de toutes les factures.
- 7.12.6 En plus d'une facture mensuelle, l'entrepreneur doit soumettre un fichier de facturation détaillé en format PDF, conformément aux indications de l'annexe E, Format du fichier de facturation.
- 7.12.7 L'entrepreneur doit soumettre le fichier de facturation détaillé chaque mois et y inclure toutes les données traitées pendant la période de facturation précédente (y compris les frais présentés à nouveau pour des périodes de facturation antérieures). Le montant figurant sur la version imprimée de la facture sommaire doit correspondre au total figurant dans le fichier de facturation détaillé. En cas de divergence, le montant du fichier prévaut. Ainsi, c'est le montant total figurant dans le fichier, moins le montant des transactions qui auront été refusées, qui sera payé.

7.13 Attestations

- 7.13.1 Le respect des attestations fournies par l'entrepreneur avec sa soumission est une condition du marché et pourra faire l'objet d'une vérification par le Canada pendant toute la durée du marché. En cas de manquement à toute déclaration de la part de l'entrepreneur ou si on constate que les attestations qu'il a fournies avec sa soumission comprennent de fausses déclarations, faites sciemment ou non, le Canada aura le droit de résilier le marché pour manquement conformément aux clauses du marché en la matière.

7.14 Lois applicables

Le contrat doit être interprété et régi, et les relations entre les parties doivent être déterminées, par les lois en vigueur en _____. < À insérer au moment de l'attribution du contrat >

7.15 Ordre de priorité des documents

En cas de divergence entre le libellé des textes énumérés dans la liste qui suit, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste :

- 7.15.1 Section 02 des conditions générales 4005 (Services et produits de télécommunications) intitulée « Droits de résiliation relatifs à l'inobservation des garanties et déclarations relatives aux télécommunications »;
- 7.15.2 _____ (collectivement appelés le « **tarif** »)

Remarque à l'intention des soumissionnaires : La présente clause ne sera pas intégrée au contrat subséquent si la soumission de l'entrepreneur n'est pas assujettie à des tarifs.

- 7.15.3 les articles de cette convention, ainsi que les différentes clauses du guide des CUA qui sont intégrées par renvoi dans ce marché;
- 7.15.4 les Conditions générales supplémentaires 4005, à l'exception de la section 2, qui l'emporte comme l'indique le sous-paragraphe ci-dessus 7.15.1;
- 7.15.5 les Conditions générales 2035 (07-16-2012), Conditions générales – besoins plus complexes de services;
- 7.15.6 l'annexe A, Énoncé des travaux;
- 7.15.7 l'annexe B – Prix des SII
- 7.15.8 l'annexe C – Liste de vérification des exigences relatives à la sécurité;
- 7.15.9 l'annexe D, Accès aux biens de l'État pour les services de télécommunications;
- 7.15.10 l'annexe E, Format du fichier de facturation
- 7.15.11 les commandes de services signées;

7.16 R ressortissants étrangers (entrepreneur canadien)

- 7.16.1 Clause A2000C (2006-06-16) du Guide des CUA, R ressortissants étrangers (entrepreneur canadien)

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

7.17 R ressortissants étrangers (entrepreneur étranger)

- 7.17.1 Clause du Guide des Clauses et conditions uniformisées d'achat A2001C (2006-06-16), R ressortissants étrangers (entrepreneur étranger)

7.18 Exigences en matière d'assurance

- 7.18.1 Clause du guide des CUA G1005C (2008-05-12) - Assurances

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

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

7.19.2 Responsabilité de la première partie

- 7.19.2.1 L'entrepreneur est entièrement responsable envers le Canada de tous les dommages, y compris les dommages indirects, particuliers et consécutifs, causés par l'exécution ou l'inexécution du marché par l'entrepreneur et qui se rapportent à :
 - 7.19.2.1.1 toute violation des droits de propriété intellectuelle dans la mesure où l'entrepreneur viole l'article des conditions générales intitulé « Atteinte aux droits de propriété intellectuelle et redevances »;
 - 7.19.2.1.2 toute blessure physique, y compris la mort.

- 7.19.2.2 L'entrepreneur est entièrement responsable de tous les dommages directs aux biens personnels matériels ou tangibles qui sont la propriété du Canada, en sa possession, ou qui sont occupés par le Canada.
- 7.19.2.3 Chaque partie est responsable de tous les dommages directs causés par son manquement à l'obligation de confidentialité en vertu du contrat. Chaque partie est aussi responsable de tous les dommages indirects, particuliers ou consécutifs relatifs à sa divulgation non autorisée des secrets industriels de l'autre partie (ou des secrets industriels d'un tiers fournis par une partie à une autre, en vertu du contrat) qui concernent la technologie de l'information.
- 7.19.2.4 L'entrepreneur est responsable de tous les dommages directs qui se rapportent à une charge ou à une réclamation liée à toute portion des travaux pour lesquels le Canada a effectué un paiement. Cette clause ne s'applique pas aux engagements ou aux réclamations relatives aux droits de propriété intellectuelle, lesquelles sont traitées au sous-paragraphe 7.17.2.1.1 ci-dessus.
- 7.19.2.5 L'entrepreneur est aussi responsable des autres dommages directs qu'il a causés au Canada relativement au marché, y compris :
- 7.19.2.5.1 tout manquement aux obligations en matière de garantie dans le cadre du contrat, jusqu'à concurrence du coût total payé par le Canada (y compris toute taxe applicable) pour les biens et les services touchés par le manquement;
- 7.19.2.5.2 tout autre dommage direct, y compris tous les coûts directs identifiables engagés par le Canada pour faire appel à une autre partie pour effectuer les travaux lorsque le contrat est résilié en totalité ou en partie pour manquement, jusqu'à concurrence d'un maximum global pour le présent sous-paragraphe 7.17.2.5.2 correspondant au montant le plus élevé entre 25 % du coût total estimatif (le montant en dollars inscrit sur la première page du contrat dans la case intitulée « Coût total estimatif », ou indiqué sur chaque commande subséquente à une offre à commandes, bon de commande ou tout autre document utilisé pour commander des biens ou des services dans le cadre du présent instrument) et 1 000 000 \$.
- 7.19.2.5.3 Dans tous les cas, la responsabilité totale de l'entrepreneur prévue au sous-paragraphe 7.17.2.5 ne dépassera pas le coût total estimatif (comme il est défini ci-dessus) du contrat ou 1 000 000 \$, le montant le plus élevé étant retenu.
- 7.19.2.6 Si les dossiers ou les données du Canada sont endommagés à la suite d'une négligence ou d'un acte délibéré de l'entrepreneur, la seule responsabilité de l'entrepreneur consiste à rétablir à ses frais les dossiers et les données du Canada en utilisant la copie de sauvegarde la plus récente conservée par le Canada. Ce dernier doit s'assurer de sauvegarder adéquatement ses documents et données.

7.19.3 Réclamations de tiers

- 7.19.3.1 Que la réclamation soit faite au Canada ou à l'entrepreneur, chaque partie convient qu'elle est responsable des dommages qu'elle cause à tout tiers relativement au marché, tel que stipulé dans un accord de règlement ou ultimement déterminé par une cour compétente, si la cour détermine que les parties sont conjointement et solidairement responsables ou qu'une seule partie est uniquement et directement responsable envers le tiers. Le montant de la responsabilité sera celui précisé dans l'accord de règlement ou déterminé par la cour comme ayant été la portion des dommages que la partie a causés au tiers. Aucun accord de règlement ne lie une partie, sauf si ses représentants autorisés l'ont approuvé par écrit.
- 7.19.3.2 Si le Canada doit, en raison d'une responsabilité conjointe et solidaire, payer un tiers pour des dommages causés par l'entrepreneur, ce dernier doit rembourser au Canada le montant ultimement déterminé par une cour compétente comme étant la portion de l'entrepreneur des dommages qu'il a lui-même causés au tiers. Toutefois, malgré le sous-paragraphe 7.17.3.1, en ce qui concerne les dommages-intérêts spéciaux, indirects ou consécutifs subis par des tiers et couverts par le présent article, l'entrepreneur est uniquement responsable de rembourser au Canada sa portion des dommages que le Canada doit payer à un tiers sur ordre d'une cour, en raison d'une responsabilité conjointe et solidaire relativement à la

violation des droits de propriété intellectuelle; de blessures physiques à un tiers, y compris la mort; des dommages touchant les biens personnels matériels ou immobiliers d'un tiers; tout engagement ou toute réclamation sur toute portion des travaux; ou du manquement à l'obligation de confidentialité.

- 7.19.3.3 Les parties sont uniquement responsables l'une devant l'autre des dommages causés à des tiers dans la mesure décrite au présent sous-paragraphe 7.17.3.3.

7.20 Entrepreneur en coentreprise

- 7.20.1 L'entrepreneur confirme que le nom de la coentreprise est _____ et que cette dernière est constituée des membres suivants :
- 7.20.2 En ce qui a trait aux rapports entre les membres de cette coentreprise, chacun d'eux adopte les conventions, fait les déclarations et offre les garanties suivantes (le cas échéant) :
- 7.20.2.1 _____ a été nommé comme « membre représentant » de la coentreprise et est pleinement habilité à intervenir à titre de mandataire de chacun des membres de cette coentreprise pour ce qui est de toutes les questions liées à ce contrat;
- 7.20.2.2 en informant le membre représentant, le Canada sera réputé avoir également informé tous les membres de cette coentreprise;
- 7.20.2.3 toutes les sommes versées par le Canada au membre représentant seront réputées avoir été versées à tous les membres.
- 7.20.3 Tous les membres conviennent que le Canada peut, à sa discrétion, résilier le marché en cas de conflit entre les membres qui, de l'avis du Canada, nuit d'une manière ou d'une autre à l'exécution des travaux.
- 7.20.4 Tous les membres de la coentreprise sont conjointement et séparément ou solidairement responsables de l'exécution de la totalité de ce marché.
- 7.20.5 L'entrepreneur reconnaît que toute modification apportée à la composition de la coentreprise (soit un changement dans le nombre de ses membres ou le remplacement d'un membre par un autre) constitue une affectation et est soumise aux clauses pertinentes des conditions générales du marché.
- 7.20.6 L'entrepreneur reconnaît que, le cas échéant, toutes les exigences contractuelles relatives aux marchandises contrôlées et à la sécurité s'appliquent à chaque membre de la coentreprise.

Remarque à l'intention des soumissionnaires : Cet article sera supprimé si le soumissionnaire auquel le marché est adjugé n'est pas une coentreprise. Si l'entrepreneur est une coentreprise, cet article sera complété à l'aide de l'information contenue dans sa soumission.

7.21 Services de télécommunications

- 7.21.1 **Améliorations apportées au service :** L'entrepreneur convient d'aviser le responsable technique de toutes les améliorations qui toucheront les services, y compris les améliorations techniques, administratives, commerciales ou tout autre type d'améliorations. L'entrepreneur accepte d'offrir sans frais au Canada toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier. Toute autre amélioration doit uniquement être fournie suivant l'approbation écrite de l'autorité contractante. On en négociera le prix au cas par cas. Ces améliorations peuvent comprendre, entre autres, les rabais résultant du regroupement de certains services ou les prix réduits pour l'ajout de capacité.

7.22 Mise en place des installations de télécommunications dans les immeubles du Canada

Les biens, les installations, le matériel, la documentation et le personnel du Canada ne sont pas forcément à la disposition de l'entrepreneur. Si ce dernier doit avoir accès aux biens, aux installations, au matériel, aux documents ou au personnel du Canada, il doit en faire la demande au responsable technique. Le Canada

permettra à l'entrepreneur d'accéder aux biens uniquement pour mettre en place le matériel et les installations de télécommunications (comme le câblage) qui sont raisonnablement nécessaires pour fournir les services au Canada selon le contrat, conformément à l'annexe « Accès aux biens de l'État pour les services de télécommunications ». L'accès à certains immeubles peut être soumis à des exigences supplémentaires en matière de sécurité. Le Canada n'est aucunement tenu de prendre des dispositions pour que l'entrepreneur puisse accéder aux immeubles qui n'appartiennent pas à l'État. Il ne lui incombe pas non plus de payer les droits d'accès demandés par tout autre propriétaire.

7.23 Préservation des supports électroniques

- 7.23.1 L'entrepreneur doit soumettre à la détection électronique, à l'aide d'un progiciel mis à jour à intervalles réguliers, l'ensemble des supports électroniques utilisés dans l'exécution des travaux, en vue de détecter des virus électroniques et d'autres codes visant à causer des défauts, avant de s'en servir sur l'équipement du Canada. Il devra informer aussitôt le Canada si un support électronique utilisé dans le cadre des travaux renferme des virus informatiques ou d'autres codes visant à causer des défauts.
- 7.23.2 Si des renseignements ou des documents électroniques sont endommagés ou perdus pendant qu'ils se trouvent sous la garde de l'entrepreneur ou avant d'être livrés au Canada conformément au marché, y compris en cas d'effacement accidentel, l'entrepreneur doit les remplacer immédiatement, à ses frais.

7.24 Déclarations et garanties

L'entrepreneur a fait des déclarations à propos de son expérience et de son expertise dans sa soumission qui a donné suite à l'attribution du contrat. L'entrepreneur déclare et certifie que toutes ces déclarations sont exactes et reconnaît que le Canada s'est fondé sur celles-ci pour lui adjuger ce marché. De plus, l'entrepreneur déclare et certifie qu'il a, et qu'il aura pendant la durée du contrat, ainsi que tout le personnel et les sous-traitants qui effectueront les travaux, les compétences, l'expérience et l'expertise nécessaires pour mener à bien les travaux conformément aux tâches décrites dans le contrat et qu'il a (ainsi que le personnel et les sous-traitants) déjà rendu de pareils services à d'autres clients.

7.25 Services de transition à la fin de la période visée par le contrat

L'entrepreneur convient qu'au cours de la période menant à la fin de la durée du contrat, il déploiera tous les efforts raisonnables pour aider le Canada pendant la transition entre ce contrat et le nouveau contrat conclu avec un autre fournisseur. L'entrepreneur convient qu'il ne facturera aucuns frais pour ces services.

ANNEXE A
ÉNONCÉ DES TRAVAUX

<Ci-joint>

ANNEXE B

Prix des Services d'interconnexion Internet (SII)

< À insérer au moment de l'attribution du contrat >

ANNEXE D

ACCÈS AUX BIENS DE L'ÉTAT AUX FINS DES SERVICES DE TÉLÉCOMMUNICATIONS

1. ACCÈS

1.1. Salle d'équipement et utilisation

1.1.1. Pour la durée du contrat, le Canada accorde à l'entrepreneur l'accès aux biens de l'État aux fins suivantes :

1.1.1.1. Installer, entretenir, exploiter, réparer, remplacer et enlever, aux frais et aux risques de l'entrepreneur seulement, l'« **équipement de communication** » (qui comprend les armoires, les bâtis et d'autres équipements électroniques mentionnés à l'appendice A) sur et dans la salle d'équipement (tel qu'il est décrit à l'appendice B) sur les terrains et dans les bâtiments (la « **propriété** ») désignés dans le contrat en vue de la prestation des services de télécommunications;

1.1.1.2. Installer, entretenir, exploiter, réparer et remplacer, aux frais et aux risques de l'entrepreneur seulement, l'« **équipement de raccordement** » (qui comprend les câbles, les conduits, les doublures de conduit, le matériel de raccordement et autre équipement passif, conformément à l'appendice A). L'entrepreneur a également le droit de faire passer l'équipement de raccordement dans le « **maillon d'entrée** » (correspondant au maillon principal de pénétration dans les fondations de la propriété) et dans d'autres « **espaces de communication de la propriété** » (correspondant aux voies de télécommunications requises pour passer du maillon d'entrée à la salle d'équipement de l'entrepreneur située dans le bâtiment et de cette salle d'équipement aux clients de l'entrepreneur, comme il s'avère nécessaire pour fournir les services de télécommunications aux clients de l'entrepreneur, désignés et approuvés par le Canada). L'ensemble de l'équipement de communication et de raccordement de l'entrepreneur sont désignés l'« **équipement de l'entrepreneur** », et le maillon d'entrée, les espaces de communication de la propriété et la salle d'équipement sont désignés l'« **aire d'accès** »;

1.1.1.3. Utiliser le câblage de télécommunication existant du Canada, s'il est disponible, conformément aux lignes directrices du CRTC les plus récentes (ou, en l'absence de lignes directrices du CRTC, conformément aux pratiques exemplaires de l'industrie) relatives à l'utilisation du câblage de même type, afin de raccorder l'équipement de l'entrepreneur aux utilisateurs se trouvant dans la propriété. Le Canada peut autoriser l'utilisation du maillon d'entrée et du câblage existants dans la propriété pour autant qu'il soit propriétaire de ces installations et qu'il ait l'autorité d'en permettre l'utilisation. En aucun cas, le Canada n'aura l'obligation de fournir à l'entrepreneur l'utilisation d'installations alors qu'il ne possède ni ne contrôle ces installations ou qu'il n'a pas l'autorité d'en permettre l'utilisation;

1.1.1.4. le droit d'entrée et de sortie des employés, des agents, des clients et des invités de l'entrepreneur ainsi que le droit d'utilisation des ascenseurs, des halls d'entrée, des passages, des escaliers, des voies d'accès, des aires communes de chargement et d'arrêt de l'équipement dans la propriété ou à proximité (les « **aires d'équipement communes** »).

1.1.2. Le Canada fournira la surface utile située dans un endroit qu'il aura désigné dans la propriété et qui correspond à la zone ombrée du plan d'étage figurant à l'appendice B de la présente annexe (la « **salle d'équipement** »). Le Canada a le droit, à sa seule discrétion, de limiter de manière raisonnable le type, la taille et l'emplacement de l'équipement de l'entrepreneur se trouvant dans la propriété.

- 1.1.3. L'accès accordé n'est pas exclusif. Le Canada a le droit d'accorder, de renouveler et d'étendre les mêmes droits à d'autres.
- 1.1.4. L'entrepreneur doit utiliser l'aire d'accès uniquement dans le but de fournir les services de télécommunications au Canada (« **utilisation permise** »). Il est expressément interdit à l'entrepreneur de desservir d'autres propriétés ou d'autres clients à partir de cet emplacement sans obtenir au préalable l'autorisation écrite du Canada. Des conditions et des frais supplémentaires pourraient s'appliquer, selon l'entente entre les parties, concernant l'utilisation de la salle d'équipement de l'entrepreneur comme point de service pour d'autres propriétés situées à l'extérieur de la propriété de l'État.
- 1.1.5. L'entrepreneur reconnaît que, en vertu de ces dispositions, il ne peut ni ne doit réclamer à quelque moment que ce soit des intérêts ou des droits quels qu'ils soient ou dans quelque mesure que ce soit concernant la propriété, les espaces de communication ou la salle d'équipement, ou concernant l'utilisation de la propriété, des espaces de communication ou de la salle d'équipement. L'entrepreneur reconnaît également que, en aucun cas, les relations entre le Canada et l'entrepreneur ne seront considérées comme des relations de propriétaire et de locataire et que, en aucun cas, l'entrepreneur ne sera autorisé à se prévaloir des droits accordés aux locataires en vertu des lois de la province qui régissent le contrat.

1.2. Inspection

Le Canada ne donne aucune garantie ni ne fait aucune déclaration indiquant que l'aire d'accès ou la propriété conviennent à l'utilisation qu'en fera l'entrepreneur. Par conséquent, l'entrepreneur reconnaît et accepte que l'accès à la salle d'équipement soit fourni tel quel, dans les conditions existantes. Il n'existe pas de convention, d'entente, de promesse, de déclaration, de garantie, de condition ou d'engagement, explicite ou implicite, accessoire ou autre, oralement ou par écrit, établi par le Canada ou par un agent, un représentant ou toute autre personne liée au Canada, relativement au zonage, à l'utilisation, au développement, à la transformation ou à la décoration d'une partie ou de l'ensemble de l'aire d'accès ou relativement à l'installation d'équipement ou d'accessoires fixes dans une partie ou l'ensemble de l'aire d'accès, à moins que ce soit clairement établi dans les présentes dispositions.

1.3. Garantie de l'entrepreneur

L'entrepreneur garantit que l'exploitation de l'équipement de l'entrepreneur ne nuira pas à l'exploitation de l'équipement radio ou de télécommunication existant dans la propriété, ni à l'utilisation et à la jouissance de la propriété par tout autre occupant de la propriété, ses employés, ses clients et ses invités. Si l'exploitation de l'équipement de l'entrepreneur nuit à l'exploitation de l'équipement radio ou de télécommunication existant dans la propriété et que l'entrepreneur ne réussit pas à remédier à la situation dans les 24 heures suivant l'avis du Canada, celui-ci peut alors, en plus de ses droits découlant de la clause 4.2 des présentes dispositions, entrer dans la salle d'équipement et corriger ce qui cause l'interférence, et l'entrepreneur doit verser au Canada les coûts associés à cette intervention en plus d'une somme équivalant à 15 % des coûts et représentant les frais généraux du Canada.

1.4. Gestion des télécommunications

- 1.4.1. L'entrepreneur reconnaît et accepte que le Canada a le droit, mais non l'obligation, de coordonner, de restreindre, de renforcer et d'approuver l'accès de toute entreprise de gestion voulant accéder aux colonnes montantes du bâtiment. L'entrepreneur reconnaît que le Canada peut employer les services d'une entreprise de gestion pour coordonner, superviser et approuver les travaux des entrepreneurs en télécommunication, aux frais du Canada à moins d'indication contraire dans les présentes dispositions ou selon une entente préalable avec l'entrepreneur.
- 1.4.2. L'entrepreneur reconnaît que le Canada puisse vouloir fournir un accès aux fournisseurs de services de télécommunications avec lesquels les locataires de la propriété font ou feront affaire, et que le Canada puisse trouver souhaitable d'atteindre cet objectif grâce à l'utilisation commune

d'une partie ou de l'ensemble des espaces de communication de la propriété. Le Canada peut acheter certaines parties de l'équipement de l'entrepreneur (à l'exception du câblage) qu'il considère, à sa seule discrétion, comme nécessaire pour assurer l'efficacité au sein des espaces de communication de la propriété. Le Canada reconnaît que l'entrepreneur peut être lié par des ententes de service avec des clients se trouvant dans la propriété qui l'obligent à garder la propriété de l'équipement de raccordement, de sorte que l'entrepreneur ne peut être obligé de vendre ces parties de son équipement de raccordement. Le prix d'achat des parties de l'équipement de raccordement de l'entrepreneur sera déterminé en fonction de la fraction non amortie du coût en capital au moment où le Canada émet un avis d'achat par écrit. En ce qui concerne un tel achat, le Canada accepte de négocier les conditions du contrat afin de permettre l'utilisation continue de l'équipement de raccordement vendu, à un prix correspondant à sa juste valeur marchande. »

- 1.4.3. Si le Canada veut acheter le câblage qui fait partie de l'équipement de raccordement, il en négociera les conditions d'achat avec l'entrepreneur.

1.5. Accès

L'entrepreneur peut accéder à l'aire d'accès seulement en vertu des présentes dispositions et en accord avec les instructions du gestionnaire immobilier responsable de la propriété. L'entrepreneur reconnaît et accepte que ses représentants ou sous-traitants puissent devoir obtenir l'attestation de sécurité appropriée avant d'accéder à l'aire d'accès. L'entrepreneur peut accéder à l'aire d'accès 24 heures sur 24, 7 jours sur 7, pour autant qu'il en avise le Canada au préalable aussi tôt que possible. Lorsque l'entrepreneur requiert un accès avant 8 heures ou après 18 heures, du lundi au vendredi, ou en tout temps, le samedi, le dimanche ou durant un jour férié, il doit payer, à moins d'indication contraire du Canada, des frais supplémentaires selon le tarif horaire convenu conformément à la directive de TPSGC sur les tarifs horaires facturables et, le cas échéant, selon les modifications effectuées, en vigueur à la date de la convention d'accès.

2. COÛTS SUPPLÉMENTAIRES

2.1. Coûts des autres services

- 2.1.1. L'entrepreneur doit payer au Canada tous les frais associés à la prestation de services supplémentaires liés à l'installation et à l'exploitation de l'équipement de communication, tel que le Canada l'aura déterminé de façon raisonnable selon les besoins. Ces frais peuvent inclure, sans s'y limiter, les frais de services publics supplémentaires ainsi que les frais pour assurer la sécurité, la supervision, la réception, le stockage, la manutention et le déplacement des matériaux et des articles. Si l'entrepreneur en fait la demande par écrit, le Canada fournira une estimation des coûts avant que les services soient fournis ou exécutés aux frais de l'entrepreneur. Si le Canada juge bon de ne pas fournir ces services à l'entrepreneur, ils devront être fournis uniquement par les personnes que le Canada aura approuvées par écrit de manière raisonnable.
- 2.1.2. À moins d'une indication contraire acceptée par le Canada et l'entrepreneur, celui-ci doit payer le coût de tous les travaux, matériaux et autres services exécutés ou fournis par le Canada relativement à la salle d'équipement, en plus des frais d'administration de 15 %. De plus, si le Canada détermine de manière raisonnable que d'autres services sont requis, l'entrepreneur doit verser au Canada tous les frais pour tous les autres services, que ces services particuliers aient ou non été requis par l'entrepreneur. Le Canada transmettra un avis dans un délai raisonnable avant de fournir ou d'exécuter ces services.

2.2. Paiement

L'entrepreneur paiera au Canada, dans les 30 jours suivant la réception des factures, tous les montants exigés conformément aux présentes dispositions, sinon on considérera qu'il ne se conforme pas au

contrat. Tous les montants en souffrance, dus par l'entrepreneur, porteront intérêt à compter de la date où ces montants sont dus et jusqu'à la date de paiement, au même taux que les paiements dus par le Canada à l'entrepreneur en vertu de la clause intitulée « Intérêt sur les comptes en souffrance » des Conditions générales.

3. CONSTRUCTION ET MAINTENANCE

3.1. Construction

- 3.1.1. Sous la supervision constante du Canada, l'entrepreneur doit installer à ses frais son équipement (s'il y a lieu), y compris les accessoires de canalisation, les ancrages et autres matériaux utilisés pour fixer l'équipement de l'entrepreneur à l'aire d'accès; préparer la salle d'équipement et effectuer les travaux supplémentaires décrits à la section 3.1.3; l'ensemble de ces travaux est désigné collectivement « **travaux d'installation** ». Les travaux d'installation doivent être de nature, de qualité et de conception professionnelles, et ils sont assujettis à l'approbation écrite préalable du Canada. L'entrepreneur doit effectuer les travaux d'installation ainsi que fournir et installer l'équipement de communication conformément aux plans, aux dessins et aux devis qu'il aura soumis à l'avance au Canada afin d'obtenir son approbation écrite préalable. En aucun cas, l'approbation de ces plans par le Canada ne sera considérée comme une déclaration indiquant que l'équipement de l'entrepreneur ne perturbera pas les autres systèmes de la propriété ou que les plans de l'entrepreneur se conforment aux lois, aux règlements et aux règles applicables, étant donné que cette responsabilité incombe toujours à l'entrepreneur.
- 3.1.2. Les travaux d'installation doivent être exécutés : (i) aux frais de l'entrepreneur seulement; (ii) par des entrepreneurs et des travailleurs approuvés par le Canada; (iii) selon les règles de l'art appropriées; (iv) conformément aux dessins et aux devis approuvés par le Canada; (v) conformément à l'ensemble des lois et des règlements applicables; (vi) et assujettis aux règles, à la supervision, au contrôle et à l'inspection du Canada exercés de manière raisonnable; (vii) assujettis aux dédommagements par rapport aux privilèges et aux dépenses requis raisonnablement par le Canada. À l'achèvement des travaux d'installation et de tous travaux de réparation futurs, l'entrepreneur doit fournir, à ses frais, au Canada un ensemble complet de plans conformes à l'exécution, y compris leurs versions électroniques, portant sur les systèmes mécaniques et électriques, l'architecture et la structure de la salle d'équipement. L'entrepreneur doit rembourser au Canada les frais raisonnablement engagés par l'État pour revoir les plans et devis et superviser tous les travaux à cet égard. Nonobstant les dispositions précédentes, le Canada aura le droit d'exécuter, aux frais de l'entrepreneur, tout travail d'installation associé au bâtiment, et l'entrepreneur doit rembourser au Canada les coûts de ces travaux en plus d'une somme équivalant à 15 % de ces coûts et représentant les frais généraux du Canada, le tout étant déterminé de manière raisonnable par le Canada.
- 3.1.3. L'entrepreneur doit, à ses frais, obtenir tous les permis, accès, consentements et autres approbations requis, le cas échéant, pour l'installation, la maintenance et l'exploitation de l'équipement de l'entrepreneur. Lorsque le Canada l'exige, l'entrepreneur doit obtenir d'un ingénieur professionnel l'assurance écrite que les travaux d'installation se conforment à toutes les mesures de sécurité requises, y compris la résistance à la charge du vent et la capacité de chargement du plancher.
- 3.1.4. Pour toutes les nouvelles installations, l'entrepreneur doit étiqueter chaque câble introduit dans les voies de télécommunication, dans chaque poste téléphonique où passent les câbles, en indiquant les renseignements d'identification, y compris, mais sans s'y limiter, le numéro de série du contrat, l'étage d'où provient le câble et l'étage où il se termine ainsi que tout autre renseignement raisonnablement requis par le Canada.
- 3.1.5. Durant les travaux de construction ou autrement, l'entrepreneur ne bloquera pas l'accès aux quais de chargement de la propriété, aux trottoirs l'entourant ni à aucune des entrées et n'empêchera pas ni ne gênera de quelque façon que ce soit leur utilisation. Si cela arrive,

l'entrepreneur doit prendre les mesures correctives aussi rapidement que possible, mais pas plus tard que 24 heures après l'avis du Canada à cet effet.

- 3.1.6. L'entrepreneur peut modifier l'appendice A au besoin, pour autant qu'il obtient au préalable le consentement écrit du Canada. Ce consentement ne doit pas être refusé de manière déraisonnable afin de répondre aux besoins des autres locataires. Toutes les conditions stipulées à la clause 3 s'appliqueront à de telles circonstances. L'entrepreneur a l'entière responsabilité des coûts relatifs à la construction de toute installation supplémentaire, y compris mais sans s'y limiter les colonnes montantes et les salles de télécommunication, lorsque c'est nécessaire en vue de l'installation de l'équipement de l'entrepreneur.
- 3.1.7. Le Canada peut : (i) modifier, aménager et construire des installations supplémentaires dans la propriété et apporter des améliorations à la propriété; (ii) déplacer les installations et les améliorations dans la propriété; (c) faire tout ce qui est nécessaire dans ou sur la propriété pour se conformer aux lois, aux règlements, aux normes, aux ordonnances ou aux directives concernant une partie ou l'ensemble de la propriété; (d) faire dans ou sur la propriété tout ce qu'il considère comme utile.

3.2. Matières dangereuses

- 3.2.1. L'entrepreneur n'installera ni n'apportera aucune substance ou matière dangereuse dans la propriété. Si des matières dangereuses sont installées ou apportées dans la propriété par l'entrepreneur ou en son nom, il doit les enlever dans les 24 heures. Si l'entrepreneur trouve ou expose de quelque manière que ce soit des matières dangereuses dans la propriété, il doit immédiatement arrêter les travaux en cours et signaler ses découvertes au Canada dans les 24 heures. L'entrepreneur ne doit pas effectuer d'autres travaux dans la salle d'équipement concernée sans obtenir au préalable l'approbation écrite du Canada.
- 3.2.2. Trois possibilités s'offrent à l'entrepreneur qui découvre la présence de matières dangereuses et cesse les travaux comme il est indiqué précédemment : (i) modifier la voie d'accès planifiée afin d'éviter les salles d'équipement contenant des matières dangereuses; (ii) fermer l'accès à ces salles d'équipement selon la procédure décrite à la clause 4; (iii) établir un nouveau calendrier des travaux d'installation à mettre en œuvre une fois que les mesures correctives prises par le Canada sont terminées; toutefois, l'entrepreneur peut mettre fin à l'utilisation de l'aire d'accès en donnant un avis écrit au Canada si les mesures correctives ne sont pas entreprises ou exercées avec diligence dans les 30 jours après que le Canada a reçu l'avis de l'entrepreneur l'informant de la présence de matières dangereuses. Si le point (i) n'est pas possible ou si le point (iii) entraîne des délais dans les travaux d'installation, l'entrepreneur est dégagé de l'obligation de fournir les services de télécommunication nécessitant l'utilisation de l'aire d'accès concernée.

3.3. Entretien et réparation

- 3.3.1. La maintenance, les réparations ou le remplacement de l'équipement de l'entrepreneur ainsi que des accessoires de canalisation, des ancrages et d'autres matériaux utilisés pour fixer l'équipement de l'entrepreneur à l'aire d'accès doivent être effectués par l'entrepreneur à ses frais et relèveront de son entière responsabilité.
- 3.3.2. À l'exception de la maintenance, des réparations ou des remplacements mentionnés à la section 3.3.1 ci-dessus, les travaux de maintenance, de réparation ou de remplacement (y compris les travaux de construction, majeurs ou non) de l'aire d'accès ou de toute autre partie de la propriété seront effectués par le Canada, aux frais de l'entrepreneur seulement, lorsque ces travaux sont rendus nécessaires en raison : (i) de l'utilisation de l'aire d'accès par l'entrepreneur, (ii) de l'installation ou de l'exploitation de l'équipement de l'entrepreneur ou (iii) de l'installation de tout câblage relié à l'équipement de l'entrepreneur.

- 3.3.3. Lorsque (i) la propriété est endommagée ou détruite, ou que des réparations, des remplacements ou des modifications à la propriété sont nécessaires à la suite d'une action ou d'une omission de l'entrepreneur, de ses employés, de ses agents, de ses invités, de ses permissionnaires, de ses entrepreneurs ou d'autres personnes envers qui il est légalement responsable; ou que (ii) le Canada détermine que les réparations, les remplacements ou les améliorations à une partie de la propriété, y compris sans s'y limiter à l'un des systèmes de la propriété, sont requis à la suite de l'utilisation de l'aire d'accès par l'entrepreneur, celui-ci doit verser au Canada le coût de ces réparations, de ces remplacements, de ces améliorations ou de ces modifications.
- 3.3.4. Si le Canada détermine (i) que la présence de l'équipement de l'entrepreneur dans la propriété, (ii) que l'état de l'équipement de l'entrepreneur ou (iii) que l'utilisation de la propriété par l'entrepreneur crée une situation d'urgence, le Canada prendra, sans en aviser l'entrepreneur, les mesures qu'il juge nécessaires pour remédier à la situation, et l'entrepreneur devra lui verser le coût de ces mesures en plus d'une somme équivalant à 15 % de ce coût (représentant les frais généraux du Canada).

4. RÉSILIATION

4.1. Restauration de la salle d'équipement

- 4.1.1. À moins d'indication contraire dans cette clause, l'équipement de l'entrepreneur demeurera en tout temps sa propriété. À l'expiration du droit d'utilisation de l'aire d'accès ou lors de la résiliation hâtive, l'entrepreneur doit à ses frais : (i) enlever de l'aire d'accès l'équipement de l'entrepreneur, tous les accessoires fixes d'exploitation et tous les biens personnels lui appartenant, (ii) restaurer les aires d'accès selon les normes courantes du Canada relativement à la propriété (y compris mais sans s'y limiter l'enlèvement et la disposition de toute substance toxique ou dangereuse et de ses contenants conformément aux lois applicables et aux exigences des autorités ainsi que la réparation et la restauration nécessaires du toit de la propriété) dans la mesure exigée par le Canada, et (iii) remettre au Canada la possession paisible des aires d'accès (en ordre, en bonnes conditions et réparées comme l'entrepreneur est requis de le faire en vertu des présentes dispositions relatives à la maintenance et à la conservation de l'aire d'accès). L'entrepreneur doit réparer à ses frais tous les dommages causés à une partie ou à l'ensemble de la propriété à la suite de cet enlèvement ou de cette restauration.
- 4.1.2. Si l'entrepreneur n'enlève pas son équipement, les accessoires fixes d'exploitation et ses biens personnels au moment de l'expiration du droit d'utilisation de l'aire d'accès ou de la résiliation hâtive, alors le Canada, selon sa décision et sans préjudice relativement à d'autres droits ou recours dont il dispose, deviendra le propriétaire absolu de l'équipement de l'entrepreneur, des accessoires fixes d'exploitation et de ses biens personnels sans devoir verser une compensation à l'entrepreneur et sans en aviser l'entrepreneur; le Canada pourra les enlever de l'aire d'accès, les vendre ou en disposer de la façon qu'il juge utile, sans aucune responsabilité quelle qu'elle soit de sa part. Si l'entrepreneur ne réussit pas à réparer les dommages ou à terminer les travaux, l'enlèvement, la disposition ou la restauration dont il est question dans cette clause au moment de l'expiration du droit d'utilisation de l'aire d'accès ou de la résiliation hâtive, il doit verser au Canada les coûts de l'enlèvement, de la vente ou de la disposition de l'équipement, des accessoires fixes d'exploitation et des biens personnels ainsi que de la restauration de l'aire d'accès selon les normes courantes du Canada relativement à la propriété, en plus d'une somme équivalant à 15 % de ce coût et représentant les frais généraux du Canada.
- 4.1.3. L'entrepreneur reconnaît et convient explicitement que ses obligations conformément à la section 4.1.1 ci-dessus subsisteront après l'expiration du droit d'utiliser l'aire d'accès ou la résiliation et qu'elles continueront de s'imposer.

4.2. Manquement et résiliation hâtive

- 4.2.1. Si l'entrepreneur ne réussit pas à exécuter et à respecter : (i) toute disposition autre que le paiement de tous les coûts ou (ii) les règlements ou les règles, y compris leurs modifications, applicables à l'aire d'accès, le Canada pourra, en plus de ses autres droits et recours mais sans s'y limiter, suspendre immédiatement le droit d'utiliser l'aire d'accès accordé en vertu de ces dispositions en avisant l'entrepreneur par écrit (jusqu'à ce que le défaut d'exécution ou de respect soit corrigé par l'entrepreneur). Si (A) l'entrepreneur ne réussit pas à remédier à ce défaut dans les dix jours (ou une période plus courte selon ce qui est indiqué dans ces dispositions) ou si (B) le défaut ne peut raisonnablement être corrigé dans les dix jours ou moins et que l'entrepreneur ne réussit pas à commencer à remédier à ce défaut dans les dix jours ou une période plus courte ou qu'il ne réussit pas par la suite à remédier avec diligence à ce défaut, dans l'un ou l'autre cas, le Canada pourra, après l'avis de suspension indiqué à la section 4.2.1, résilier le droit d'utiliser l'aire d'accès en avisant l'entrepreneur par écrit.
- 4.2.2. Si l'entrepreneur est jugé être en défaut en vertu de la clause 2.3 de ces dispositions à la suite du défaut de paiement d'une ou des sommes dues par l'entrepreneur, le Canada peut, en avisant l'entrepreneur par écrit : (i) suspendre immédiatement le droit d'utiliser l'aire d'accès accordé à l'entrepreneur en vertu de ces dispositions (à moins que l'entrepreneur remédie à ce défaut); (ii) résilier le droit d'utiliser l'aire d'accès après les cinq jours suivant l'avis écrit de remédier au défaut; ou (iii) déduire le montant en souffrance du prochain paiement versé à l'entrepreneur en vertu du contrat.
- 4.2.3. Si l'entrepreneur abandonne l'aire d'accès ou qu'il arrête de l'utiliser aux fins permises, de manière continue et active, pendant plus de 15 jours consécutifs, le Canada pourra résilier le droit d'utiliser l'aire d'accès en avisant l'entrepreneur par écrit.
- 4.2.4. Le Canada peut en tout temps résilier le droit d'utiliser l'aire d'accès (ou une partie de celle-ci), à compter de n'importe quelle date, en envoyant un avis écrit (l'« **avis de résiliation** ») à l'entrepreneur au moins 60 jours avant la date de résiliation que l'État a désignée comme la date d'entrée en vigueur de la résiliation (la « **date de résiliation** ») et que : (i) le Canada a l'intention d'entreprendre la construction, la démolition ou le réaménagement d'une partie ou de l'ensemble de la propriété qui, selon l'opinion raisonnable l'État, sera empêché, bloqué, retardé ou gêné de quelque façon que ce soit par l'occupation de l'aire d'équipement par l'entrepreneur; (ii) le Canada a conclu une entente avec une tierce partie relativement à l'occupation de l'espace industriel, commercial, résidentiel ou de bureau situé dans la propriété, et que cette tierce partie doit utiliser une partie ou l'ensemble de l'aire d'accès; ou (iii) le Canada a entrepris de vendre une partie ou l'ensemble de la propriété incluant une partie de l'aire d'accès à un acheteur. Dans l'un ou l'autre cas, la résiliation par le Canada du droit de l'entrepreneur d'utiliser l'aire d'accès dégagera l'entrepreneur de ses obligations de fournir les services de télécommunications nécessitant l'utilisation de l'aire d'accès (ou une partie de celle-ci) à laquelle il n'aura plus accès.
- 4.2.5. Si (i) une partie de l'aire d'accès ou de la propriété est endommagée ou détruite et qu'elle ne peut pas être réparée et redevenir fonctionnelle en vue d'une utilisation normale dans les 60 jours suivant le dommage ou la destruction; ou si (ii) une partie de l'aire d'accès ou de la propriété est endommagée ou détruite à la suite d'un événement contre lequel le Canada n'est pas assuré ou qu'il n'avait pas à s'assurer ou que le coût des réparations des dommages ou de la destruction dépasse le produit de l'assurance disponible, le Canada peut par un avis écrit dans un délai de 30 jours suivant le dommage ou la destruction résilier le droit d'utiliser l'aire d'accès, et l'entrepreneur doit immédiatement remettre la possession de l'aire d'accès au Canada. Dans l'un ou l'autre cas, la résiliation par le Canada du droit de l'entrepreneur d'utiliser l'aire d'accès dégagera l'entrepreneur de ses obligations de fournir les services de télécommunications nécessitant l'utilisation de l'aire d'accès (ou une partie de celle-ci) à laquelle il n'aura plus accès.

5. DÉPLACEMENT

5.1. Déménagement

Le Canada a le droit en tout temps, en donnant un avis écrit d'au moins 60 jours (l'« **avis de déplacement** »), de déplacer l'équipement de communication et/ou de raccordement de l'entrepreneur vers d'autres locaux de la propriété (la « **nouvelle salle d'équipement** »), désignés par le Canada en concertation avec l'entrepreneur. Dans ce cas, les conditions de la présente section 5.1 s'appliqueront :

- 5.1.1. La salle d'équipement dans laquelle sera déplacé l'équipement de communication (« nouvelle salle d'équipement ») doit couvrir approximativement la même surface que la salle d'équipement originale ou être plus grande que celle-ci, et la nouvelle salle d'équipement doit, selon l'opinion raisonnable du Canada, se conformer aux exigences de l'entrepreneur relativement à l'utilisation permise.
- 5.1.2. L'entrepreneur et le Canada doivent, s'il y a lieu, partager également les frais directs raisonnables associés au déplacement de l'équipement et de tout autre matériel de l'entrepreneur contenus dans la salle d'équipement originale vers la nouvelle salle d'équipement.
- 5.1.3. Les conditions de ces dispositions s'appliquent, avec les adaptations nécessaires, à la nouvelle salle d'équipement, pour autant qu'elles soient cohérentes avec les conditions de la clause 5.1.

6. GÉNÉRALITÉS

6.1. Règles et réglementation

Conformément aux présentes dispositions, l'utilisation de la salle d'équipement et l'accès à la salle d'équipement sont assujettis aux règles et aux règlements (modifiés, le cas échéant) établis par le Canada selon les besoins.

6.2. Appendices

Les appendices A et B font partie de ces dispositions.

Appendice A de l'annexe []
Équipement de communication; Liste et spécifications
Équipement de raccordement; Liste et spécifications

[à terminer après l'attribution du contrat, s'il y a lieu]

Appendice B de l'annexe []
Salle d'équipement; Plan d'étage

[à terminer après l'attribution du contrat, s'il y a lieu]

ANNEXE E – FORMAT DU FICHER DE FACTURATION**Disposition globale du contrat (enregistrement de type 1)**

CHAMP EMPLACEMENT	NOM DU CHAMP	Taille du champ – format	DESCRIPTION D'ÉDITION
1	Type d'enregistrement	1 chiffre – Nombre entier	Type de document <<1 >> :
2 - 9	Date de la facture	8 chiffres – Date	Date d'émission de la facture, AAAAMMJJ
10 - 29	Contrat Nombre	20 caractères	Numéro de contrat unique, alignement à gauche Format - « XXXXX-YYCCCC/SSS/UU », ou Format - « XXXXXYYCCCC »
30 - 35	Période de facturation	8 chiffres (date)	Mois et année de la période de facturation, AAAAMM Cette information servira à valider la date de facturation des enregistrements de type 2. (La date doit être la même)
36 - 65	Nom de Nom	30 caractères	Nom de l'entrepreneur, alignement à gauche
66 - 77	Total des frais mensuels	12 chiffres – devise	Montant total des frais de toutes les factures du mois – (signé avec deux décimales implicites) alignement à droite
78 - 89	Total des crédits de service et des autres frais et crédits	12 chiffres – devise	Montant total des crédits de service et des autres frais et crédits pour la période – (signé avec deux décimales implicites), alignement à droite.
90 - 101	Montant total de la TVH et/ou de la TVQ	12 chiffres – Devise	Montant total de la TVH et/ou TVQ établi en fonction des frais pour la période – (signé avec deux décimales implicites), alignement à droite.
102 - 113	Montant total de la TPS	12 chiffres – Devise	Montant total de la TPS établi en fonction des frais pour la période – (signé avec deux décimales implicites) alignement à droite
114 - 125	Montant total des frais pour retard de paiement	12 chiffres – Devise	Montant total imputé pour retard de paiement pendant la période – (signé avec deux décimales implicites) alignement à droite
126 - 137	Montant total	12 chiffres – Devise	Montant total à payer établi selon la facture de l'entrepreneur pour la période – (signé avec deux décimales implicites) alignement à droite

Enregistrement de facture par numéro de compte de facturation (enregistrement de type 2)

CHAMP EMPLACEMENT	NOM DU CHAMP	TAILLE ET FORMAT DU CHAMP	DESCRIPTION D'ÉDITION
1	Type d'enregistrement	1 chiffre (nombre entier)	Type de document << 2 >> :
2 - 9	Date de la facture	8 chiffres – Date	Date d'émission de la facture, AAAAMMJJ.
10 - 19	Numéro de la facture	10 caractères	Le numéro de la facture, tel qu'il est émis par l'entrepreneur.
20 - 39	Numéro du contrat	20 caractères	Numéro de contrat unique, alignement à gauche Format - « XXXXX-YYCCCC/SSS/UU », ou Format - « XXXXXYYCCCC »
40 - 49	NCF	10 caractères	Numéro de compte de facturation
50 - 55	Période de facturation	8 chiffres - Date	L'année et le mois où la facture a été émise, AAAAMM. Cela servira à valider la date de la facture sur les enregistrements de type « 3 » (doivent être les mêmes).
56 - 85	Nom de l'entrepreneur	30 caractères	Nom de l'entrepreneur, alignement à gauche
86 - 97	Total des frais mensuels	12 chiffres –Devise	Totaux (montant récurrent + montant non récurrent) de tous les enregistrements de type 3 connexes - (signé avec deux décimales implicites) alignement à droite
98 - 109	Total des crédits de service et des autres frais et crédits	12 chiffres –Devise	Montants totaux des crédits de service et des autres frais et crédits (montant des crédits de service + autres frais et crédits par service ou circuit) de tous les enregistrements de type 3 connexes – (signé avec deux décimales implicites), alignement à droite
110-121	Montant total de la TVH et/ou de la TVQ	12 chiffres –Devise	Montant total de la TVH et/ou de la TVQ (montant cumulatif établi en fonction de tous les frais connexes de la facture) (signé avec 2 décimales implicites), alignement à droite
122-133	Montant total de la TPS	12 chiffres –Devise	Montant total de la TPS (montant cumulatif établi en fonction de tous les frais connexes de la facture) – (signé avec deux décimales implicites) alignement à droite
134-145	Montant total des frais pour retard de paiement	12 chiffres –Devise	Montant total imputé pour retard de paiement pendant la période – (signé avec deux décimales implicites), alignement à droite
146 - 157	Montant total de la facture	12 chiffres –Devise	Montant total à payer établi en fonction de tous les enregistrements de type 3 et les cumulatifs des frais connexes de la facture de l'entrepreneur – (signé avec deux décimales implicites) alignement à droite

Disposition des enregistrements pour les produits et services (enregistrement de type 3)

EMPLACEMENT DU CHAMP	NOM DU CHAMP	TAILLE ET FORMAT DU CHAMP	DESCRIPTION D'ÉDITION
1	Type d'enregistrement	1 chiffre – Nombre entier	Type de document << 3 >> :
2 - 9	Date de la facture	8 chiffres – Date	Date d'émission de la facture, AAAAMMJJ.
10 - 19	Numéro de la facture	10 caractères	Le numéro de la facture, tel qu'il est émis par l'entrepreneur.
20 - 39	Numéro du contrat	20 caractères	Numéro de contrat unique, alignement à gauche Format - « XXXXX-YYCCCC/SSS/UU », ou Format - « XXXXXYYCCCC »
40 - 49	NCF	10 caractères	Numéro de compte de facturation
50 - 84	Nom du produit	35 caractères	Nom du produit selon la convention établie par l'entrepreneur. Ce champ est obligatoire et unique au produit pour lequel cet enregistrement est fourni. (Par exemple : SII-INT-10GE-xx-ou SII-DDOS-3Gbps-xx)
85 - 112	Détails Code de produit	28 caractères	Code de circuit unique défini par l'entrepreneur (aussi appelé ID Fournisseur, pour désigner de façon unique l'élément de circuit pour l'inventaire et le suivi financier). Ce champ est obligatoire et unique au circuit pour lequel cet enregistrement est fourni. (Par exemple XOGFYFR1395)
113 - 142	Ligne d'adresse 1 de l'emplacement	30 caractères	Ligne 1 de format libre
143 - 172	Ligne d'adresse 2 de l'emplacement	30 caractères	Ligne 2 de format libre
173 - 202	Ligne d'adresse 3 de l'emplacement	30 caractères	Ligne 3 de format libre
203 - 232	Lieu (ville)	30 caractères	Nom de la ville
233 - 234	Lieu (province)	2 caractères	Abréviation officielle du nom de la province
235 - 240	Code postal de l'emplacement	6 caractères	Code postal officiel (ANANAN)
241 - 246	DPNXX	6 caractères	Indicatif régional et de central de l'emplacement du service
247 - 254	Numéro de la commande	8 caractères	Numéro d'autorisation de la commande de SPC
255 - 262	Date d'entrée en vigueur de la facturation du produit	8 chiffres – Date	Date de début de la facturation de l'entrepreneur pour le circuit, AAAAMMJJ
263 - 270	Date d'annulation de la facturation du circuit	8 chiffres – Date	Date de fin de la facturation de l'entrepreneur pour le circuit, AAAAMMJJ
271 - 280	Montant récurrent	Frais mensuels récurrents au PPS	Prix mensuel récurrent pour le circuit (vérifié en fonction des tableaux de profils des contrats) – (signé avec deux décimales implicites), alignement à droite
281 - 290	Montant unique	Frais mensuels récurrents au PPS	Prix mensuel unique pour le circuit (vérifié en fonction des tableaux de profils des contrats) – (signé avec deux décimales implicites), alignement à droite
291 - 300	Montant des crédits de service	Frais mensuels récurrents au PPS	Total des rabais et crédits pour le circuit, approuvé par le gestionnaire du service de SPC – (signé avec deux décimales implicites) alignement à droite

301 - 310	Autres frais et crédits par service ou circuit	Frais mensuels récurrents au PPS	Total des autres frais et crédits pour le service ou le circuit, approuvé par le gestionnaire de service de SPC – (signé avec deux décimales implicites) alignement à droite
311 - 320	Montant de la TVH ou de la TVQ	Frais mensuels récurrents au PPS	Montant total de la TVH ou de la TVQ calculé à partir des frais connexes du mois pour le service ou le circuit – (signé avec deux décimales implicites), alignement à droite
321 - 330	Montant de la TPS	Frais mensuels récurrents au PPS	Montant total de la TPS calculé à partir des frais connexes du mois pour le service ou circuit – (signé avec deux décimales implicites) alignement à droite
331 - 336	Période de service	8 chiffres (date)	Année et mois durant lesquels le service a été fourni et est facturé, AAAAMM

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION

Dénomination sociale du soumissionnaire : <i>[Remarque à l'intention des soumissionnaires : Il incombe aux soumissionnaires qui font partie d'une entreprise de désigner la bonne entreprise.]</i>		
Représentant autorisé du soumissionnaire aux fins de l'évaluation (p. ex. pour des précisions)	Nom	
	Titre	
	Adresse	
	Téléphone	
	Télécopieur	
	Courriel	
Numéro d'entreprise – approvisionnement (NEA) <i>[voir la clause 2003 des instructions et conditions uniformisées]</i> <i>[Remarque à l'intention des soumissionnaires : Le NEA donné doit correspondre à la dénomination sociale utilisée dans la soumission. Si ce n'est pas le cas, on établira le soumissionnaire en fonction de la dénomination sociale fournie, et le soumissionnaire devra donner le NEA qui correspond à celle-ci.]</i>		
Niveau d'attestation de sécurité du soumissionnaire <i>[indiquer le niveau et la date d'attribution]</i> <i>[Note à l'intention des soumissionnaires : assurez-vous que le nom dans l'attestation de sécurité correspond à la dénomination sociale du soumissionnaire. Si ce n'est pas le cas, l'attestation n'est pas valide pour le soumissionnaire.]</i>		
<p>En apposant ma signature ci-dessous, j'atteste, au nom du soumissionnaire, avoir lu la demande de soumissions au complet, y compris les documents qui y sont intégrés par renvoi, et que :</p> <ol style="list-style-type: none"> 1. le soumissionnaire considère avoir les compétences et que ses produits sont en mesure de satisfaire aux exigences obligatoires décrites dans la demande de soumissions; 2. cette soumission est valide pour la période indiquée dans la demande de soumissions; 3. Tous les renseignements fournis dans cette soumission sont complets et exacts; 4. si un marché est attribué au soumissionnaire, ce dernier se conformera aux modalités énoncées dans les clauses concernant le marché subséquent et comprises dans la demande de soumissions. 		
Signature du représentant autorisé du soumissionnaire		

Annexe A : Énoncé des travaux

Service d'interconnexion Internet (SII) pour Services partagés Canada (SPC)

Date : Le 4 avril 2013

Version : D11

TABLE DES MATIÈRES

1	INTRODUCTION	3
2	EXIGENCES RELATIVES AU SII	3
2.1	INFRASTRUCTURE ET TOPOLOGIE	4
2.2	PROTOCOLE BORDER GATEWAY PROTOCOL (BGP)	6
2.3	CONFIGURATION DU PIS	8
2.4	SOUTIEN POUR LA DIFFUSION GROUPÉE D'IPv4 ET D'IPv6	9
2.5	BANDE PASSANTE SUPPLÉMENTAIRE REQUISE DANS DES SITUATIONS PARTICULIÈRES	9
2.6	SERVICE DE NETTOYAGE ANTI-DÉNI DE SERVICE DISTRIBUÉ	11
3	PRÉPARATION OPÉRATIONNELLE	12
3.1	PLAN DE PRÉPARATION OPÉRATIONNELLE	12
3.2	PLAN DE GESTION DU SERVICE	13
3.3	PLAN DE CONTINUITÉ DU SERVICE	13
3.4	CONCEPTION DU SERVICE	14
3.5	DESCRIPTION DES SERVICES	14
3.6	ÉVALUATION DE LA SÉCURITÉ ET AUTORISATION (ESA)	14
3.6.1	<i>Étape 1 – ESA de la conception générale du service</i>	15
3.6.2	<i>Étape 2 – ESA de la conception de services détaillée</i>	17
3.6.3	<i>Étape 3 – Installation</i>	18
3.6.4	<i>Concept des opérations de sécurité</i>	20
3.6.5	<i>Plan de gestion des risques en matière de sécurité</i>	20
3.6.6	<i>Architecture de sécurité</i>	20
3.6.7	<i>Procédures opérationnelles de sécurité</i>	21
3.6.8	<i>Avis d'incident relatif à la sécurité</i>	21
3.6.9	<i>Plan de traitement des risques</i>	22
3.7	MISE EN ŒUVRE DU SII	22
3.7.1	<i>Réunions et rapports sur l'état d'avancement</i>	23
3.7.2	<i>Jalons de la mise en œuvre</i>	23
3.7.3	<i>Authentification, intégrité et confidentialité</i>	25
3.7.4	<i>Connectivité de réseau</i>	25
4	GESTION DU SERVICE	25
4.1	CENTRE DES OPÉRATIONS	26
4.2	CONTINUITÉ DU SERVICE	26
4.3	BUREAU DE SERVICE DU SII DE L'ENTREPRENEUR	26
4.4	FONCTIONNEMENT ET SURVEILLANCE DU SERVICE	27
4.5	ÉVALUATION DE LA SÉCURITÉ ET AUTORISATION	28
5	SERVICES DE GESTION	29
5.1	GESTION DES CHANGEMENTS	30
5.2	GESTION DE LA CONFIGURATION	32
5.3	GESTION DES INCIDENTS	33
5.4	GESTION DES VERSIONS	35
5.5	GESTION DE LA CAPACITÉ	36
5.6	GESTION DE LA DISPONIBILITÉ	36
6	RÉUNIONS	36
7	RAPPORTS ET DOCUMENTATION	37

7.1	RAPPORTS MENSUELS	38
7.2	RAPPORTS SUR DEMANDE SPÉCIALE	38
7.3	DOCUMENT SUR LA CONFIGURATION	40
8	RAPPORTS DE GESTION	41
8.1	OUTIL D'ÉCHANGE D'INFORMATION ÉLECTRONIQUE (OEIE)	41
8.2	DONNÉES SUR LE TRAFIC IP	42
8.3	RAPPORTS DE LUTTE CONTRE LE DÉNI DE SERVICE	42
8.4	PROCÉDURES DE GESTION DES OPÉRATIONS	42
8.4.1	<i>Gestion des incidents et des problèmes</i>	43
8.4.2	<i>Centre de dépannage et organisation de soutien de l'entrepreneur</i>	43
8.4.3	<i>Système et procédures de gestion des changements</i>	43
8.4.4	<i>Procédures de gestion de la sécurité</i>	43
8.5	PROCÉDURES DE GESTION DU SERVICE	43
8.6	RAPPORTS SUR LES NIVEAUX DE SERVICE	43
8.7	DEMANDES DE COMMANDE DE SERVICE	44
8.8	DOCUMENT DE CONTRÔLE D'INTERFACE (DCI)	44
8.9	SÉCURITÉ	45
8.10	EXAMEN DE LA CONFORMITÉ	45
9	GESTION DE LA QUALITÉ DU SERVICE	46
10	GESTION DES NIVEAUX DE SERVICE	46
10.1	NIVEAU DE SERVICE – ACCESSIBILITÉ À INTERNET (NS-AI)	46
10.1.1	<i>Niveau de service – Temps d'interruption maximal du service (NS-TIMS)</i>	47
10.1.2	<i>Niveau de service – Délai maximal de rétablissement du service (NS-DMRS)</i>	47
10.2	NIVEAU DE SERVICE – RÉPONSE AUX COMMANDES DE SERVICE (NS-RCS)	47
10.3	NIVEAU DE SERVICE – DÉBIT DE DONNÉES, DÉLAI DE TRANSIT ET PERTE DE PAQUETS	47
10.4	TABLEAU DES NIVEAUX DE SERVICE DU SII	48

Liste des annexes

Annexe A – Définitions et sigles

1 INTRODUCTION

- (1) Services partagés Canada (ci-après appelé « SPC ») a besoin d'un service d'interconnexion Internet (SII) qui lui permettra d'accéder aux services Internet publics pour assurer la prestation des programmes et des services offerts aux Canadiens par des ministères et organismes gouvernementaux.
- (2) Le SII a besoin de trois points d'interface de service (PIS) redondants. Ces PIS sont fournis par deux ou trois fournisseurs d'accès Internet (FAI) distincts (ci-après appelés « entrepreneur »). Consulter la figure 1 qui illustre comment chaque PIS peut traiter efficacement et de façon fiable le trafic Internet en entier, advenant une panne de ses homologues. D'autres PIS peuvent être ajoutés au SII à la demande de SPC.
- (3) SPC a configuré le réseau du Canada avec des arrangements de routage spéciaux qui permettent le réacheminement de son trafic avec le protocole Internet (IP) lorsqu'un ou plusieurs des PIS subissent une panne de service.
- (4) Dans le cours normal des opérations, tous les PIS assurent la prestation du service et chacun est prêt à prendre en charge le trafic de ses homologues advenant une panne de service chez ces derniers, le tout sans interruption.
- (5) Sauf indication contraire, le protocole IP fait référence à IPv4 et à IPv6.
- (6) L'entrepreneur doit fournir à SPC un SII, lequel comprend un service de nettoyage anti-déni de service distribué.
- (7) Les objectifs opérationnels prévoient un SII hautement fiable qui ne nécessite que des temps d'arrêt minimes pour en assurer l'entretien, de même que de courts délais de réparation.
- (8) Puisque les SII seront gérés et exploités par deux ou trois entrepreneurs distincts, ces derniers devront collaborer afin d'assurer une gestion et une exploitation transparentes, efficaces et fiables du service.
- (9) L'entrepreneur reconnaît que l'utilisation d'un portail Web fourni et géré par l'entrepreneur lui-même est la méthode privilégiée de SPC pour échanger par voie électronique de l'information de gestion et administrative, comme des dossiers d'incident, des rapports, des commandes et des factures. Cependant, d'autres solutions, tel le courriel et le transfert de fichiers, peuvent être envisagées, mais elles doivent être approuvées par SPC après l'attribution du contrat. La méthode, les outils ou le portail Web ainsi approuvés sont ci-après appelés l'Outil d'échange d'information électronique (OEIE), défini à la section 8.1.
- (10) SPC indiquera à l'entrepreneur quelles sont les personnes qui détiennent le pouvoir délégué associé à des rôles et à des responsabilités précis.
- (11) L'entrepreneur doit fournir les services du SII à SPC sur demande, en toute conformité avec les exigences de l'énoncé des travaux (EDT) et l'annexe B, Établissement des prix.

2 EXIGENCES RELATIVES AU SII

- (12) L'entrepreneur doit fournir sur commande un SII pour le réseau du Canada (GCNet) afin d'assurer une disponibilité élevée et une présence diversifiée sur Internet. Voir la figure 1 ci-dessous.

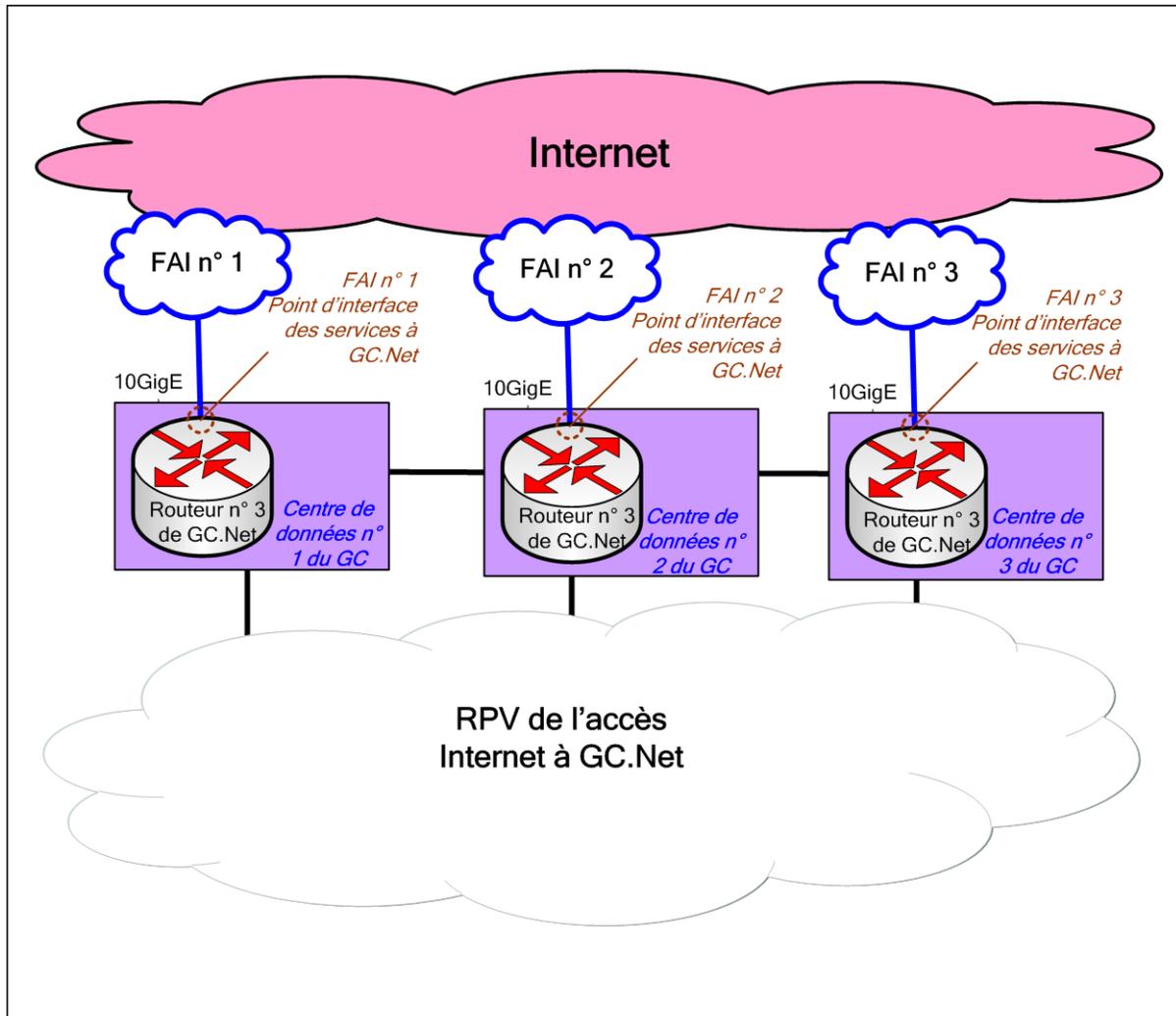


Figure 1: Infrastructure Internet du réseau du Canada

2.1 Infrastructure et topologie

- (13) Un PIS est le point de démarcation de l'entrepreneur, soit ce qui relie son SII au routeur du réseau du Canada. Le PIS du SII de l'entrepreneur est illustré dans la figure 1.
- (14) Le PIS transmet les datagrammes des versions 4 et 6 (IPv4 et IPv6) du protocole Internet en plus de tous les services de distribution de routage connexes entre le réseau du Canada et Internet, conformément au document RFC 4213. À moins d'indication contraire, les références générales au protocole IP font référence à IPv4 et à IPv6.
- (15) Les PIS du SII doivent être livrés à la demande de SPC aux centres de données du Canada, soit deux dans la région de la capitale nationale (RCN) et un dans la région de Toronto.
- (16) L'entrepreneur doit également être en mesure de fournir sur demande des PIS supplémentaires pour le SII au sein du même centre de données du Canada ou à d'autres centres de données de la RCN et de la région de Toronto.

- (17) À la demande de SPC, l'entrepreneur doit être en mesure de relocaliser un PIS du SII dans le même centre de données du Canada ou dans d'autres centres de données de la même région.
- (18) L'entrepreneur doit fournir toute l'infrastructure et tout l'équipement de réseautage nécessaires pour connecter son PIS au routeur d'interconnexion du réseau du Canada grâce à une interface de fibre Ethernet 10 Gigabit.
- (19) L'entrepreneur doit fournir au départ un débit de 4 gigabits par seconde (Gbps).
- (20) L'entrepreneur doit fournir un débit consistant en toute combinaison de trafic IPv4 et IPv6.
- (21) Le SII de l'entrepreneur doit prendre en charge les changements apportés au débit prévu de 4 Gbps à 10 Gbps, par accroissements de 1 Gbps, sans interruption de service.
- (22) Le service de l'entrepreneur doit permettre la transmission du débit convenu au départ de même qu'un débit supérieur (c.-à-d. de 4 Gbps et plus) au réseau des FAI et aux autres homologues de l'entrepreneur sur Internet, et ce, sur demande.
- (23) L'entrepreneur doit appliquer les recommandations concernant le filtrage ICMPv6 conformément au document RFC 4890, dans les cas où le réseau de l'entrepreneur achemine le trafic IPv6.
- (24) L'interface du point d'accès au réseau est l'interface du routeur de l'entrepreneur qui relie son réseau à un autre réseau sur Internet. Voir la figure 2.

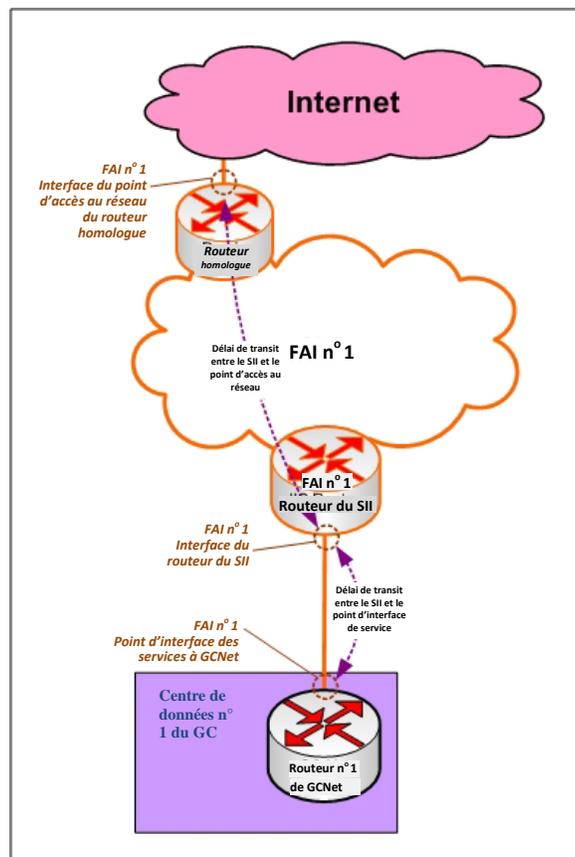


Figure 2 : Délai de transit entre le SII et le point d'accès au réseau et entre le SII et le PIS

- (25) Le SII de l'entrepreneur doit être en mesure de transmettre, lors de l'installation initiale, 4 Gbps en volume de trafic IP entre le PIS et les points d'accès au réseau de l'entrepreneur.
- (26) Dans les trente (30) jours ouvrables du gouvernement fédéral (JOGF) suivant l'adjudication du contrat, l'entrepreneur doit fournir à SPC le plan technique de la capacité et la documentation sur la conception afin de démontrer que son infrastructure et son service actuels peuvent garantir cette bande passante.
- (27) Pendant toute la durée du contrat, alors qu'augmentent les besoins relatifs à l'accès Internet, l'entrepreneur doit fournir à la demande de SPC son plus récent plan technique de la capacité et sa plus récente documentation sur la conception indiquant sa capacité à transmettre le volume croissant de trafic sur Internet tout en continuant à répondre aux exigences de l'EDT.
- (28) L'entrepreneur doit se connecter à au moins deux points d'interconnexion Internet canadiens avec les protocoles IPv4 et IPv6.
- (29) L'entrepreneur doit informer SPC de ses arrangements d'homologage et de multi-hébergement, de même que des emplacements géographiques des points d'accès au réseau.
- (30) L'entrepreneur doit aviser SPC au moins vingt (20) JOGF à l'avance de toutes les modifications apportées à ces arrangements et aux renseignements concernant les emplacements.
- (31) L'entrepreneur doit aviser SPC dans les deux (2) JOGF de toutes les modifications apportées aux ententes concernant la propriété ou la location de son infrastructure.
- (32) Les infrastructures de réseau physiques, les chemins de connexion et l'équipement de l'entrepreneur doivent être séparés et distincts afin d'obtenir un accès Internet échelonné, diversifié et insensible aux défaillances pour répondre aux besoins en matière d'interconnexion découlant des interconnexions redondantes.
- (33) Si le même entrepreneur fournit plus d'un PIS, les chemins de connexion et l'équipement, y compris les systèmes anti-déni de service distribué de chaque PIS, doivent être distincts, sauf approbation contraire de SPC.
- (34) Pour résoudre des problèmes d'interconnexion ou de performance, ou pour remplacer des composants qui ne sont plus pris en charge, SPC peut mettre à niveau de temps à autre son routeur interzone. SPC avisera l'entrepreneur concerné de toutes les mises à niveau à venir au moins trente (30) JOGF à l'avance.
- (35) L'entrepreneur doit entretenir son équipement d'interfaçage et d'infrastructure afin de respecter les niveaux de service indiqués à la section Gestion des niveaux de service.
- (36) L'entrepreneur doit s'assurer que le trafic IP n'est pas intégré dans ce service.
- (37) Sur demande, l'entrepreneur doit démontrer que le service fournit le débit nécessaire.
- (38) L'entrepreneur doit fournir tout l'équipement d'essai nécessaire pour effectuer la démonstration.

2.2 Protocole Border Gateway Protocol (BGP)

- (39) Le réseau du Canada n'est pas un système autonome (AS) de transit pour les autres fournisseurs de service Internet ou pour des réseaux autres que ceux appartenant au réseau du Canada.
- (40) Le réseau du Canada considère un réseau en aval comme un système AS de remplacement ou comme une partie du réseau du Canada en soi (c.-à-d. AS 2669). Voir la figure 3.

- (41) Le réseau du Canada effectue son propre regroupement de routages, et tient à jour ses propres renseignements de registre des routages dans la base de données Routing Arbiter Database (RADB) que l'entrepreneur doit utiliser dans la création de filtres de préfixes applicables.
- (42) Le trafic IP entre les clients du réseau du Canada ne sera pas acheminé à l'extérieur de ce réseau.

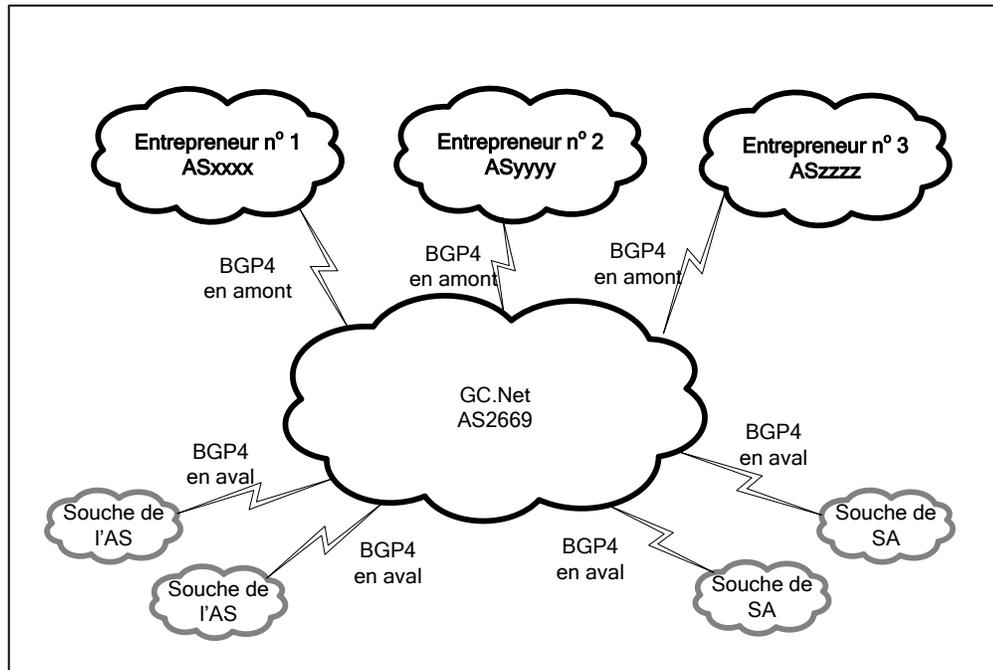


Figure 3 : Systèmes autonomes du réseau du Canada

- (43) Le SII de l'entrepreneur doit accepter le trafic IP en aval en plus des données de routage provenant du PIS.
- (44) L'entrepreneur doit prendre en charge la version 4 du protocole BGP, conformément au document RFC 4271.
- (45) L'entrepreneur doit mettre en œuvre l'approche multi-hébergement du protocole BGP utilisée par le réseau du Canada pour orienter le trafic IP vers Internet ou à partir d'Internet.
- (46) L'entrepreneur peut demander la permission de s'écarter de ces exigences ou proposer une approche de rechange, sous réserve de l'approbation de SPC.
- (47) L'entrepreneur doit fournir une connexion BGP4 externe au réseau du Canada et avoir un numéro AS unique et différent.
- (48) L'entrepreneur doit mettre en œuvre et prendre en charge les caractéristiques du protocole BGP, selon la documentation de l'Internet Engineering Task Force (IETF) au moyen des documents RFC 1772 à 1774, et des documents RFC 4760, 4893 et 4273, y compris, sans toutefois s'y limiter, ce qui suit :
- (48.a) Prise en charge de toutes les fonctions obligatoires du protocole BGP de même que des attributs bien connus.

- (48.b) Prise en charge de tous les attributs du protocole BGP de transition (c.-à-d. transfert vers un autre système AS sans modification).
- (48.c) Prise en charge de l'option d'empreinte numérique MD5 afin de protéger le protocole BGP contre les réinitialisations de session et l'injection de données malveillantes.
- (48.d) Prise en charge de multiples protocoles BGP (document RFC 4760).
- (48.e) Prise en charge des services de réseau d'accès de 32 bits.
- (49) Le SII de l'entrepreneur doit accepter les annonces de routage BGP4 provenant du service de réseau d'accès de GCNet.
- (50) Le SII de l'entrepreneur ne doit pas filtrer, rejeter ou bloquer les annonces de routage fournies par le réseau du Canada selon des critères autres que les critères suivants :
 - (50.a) Application du protocole de contrôle d'octets (BCP) 38 de l'IETF.
 - (50.b) Toute annonce de routage IPv4 avec un élément de masque supérieur à 24 bits.
 - (50.c) Toute annonce de routage IPv6 avec un élément de masque supérieur à 48 bits.
- (51) L'entrepreneur ne doit pas modifier les données de routage de GCNet sans obtenir au préalable le consentement écrit de SPC.
- (52) L'entrepreneur ne doit pas regrouper l'espace d'adresse du réseau du Canada au-delà du niveau de regroupement fourni par les annonces de routage du réseau du Canada.
- (53) Le SII de l'entrepreneur doit accepter les renseignements sur les objets de routage du réseau du Canada dans le format d'objet Routing Policy Specification Language (RPSL), comme spécifié dans les aux documents RFC 2622 et 4012.
- (54) L'entrepreneur ne doit pas mettre en œuvre le refroidissement de volet de parcours (Route Flap Dampening) conformément aux recommandations du protocole BCP 378 des Réseaux IP Européens (RIPE).
- (55) Le SII de l'entrepreneur ne doit pas accepter les demandes de changement d'annonce de réseau, les messages de courriel non formatés ou d'autres demandes ou messages dans un format semblable ou nécessitant des mécanismes similaires. L'entrepreneur doit envoyer un avis par courriel à SPC au moins un (1) JOGF suivant la réception de la demande de modifications des données de routage, et au moins deux (2) JOGF après l'application de telles modifications.
- (56) L'entrepreneur doit fournir une méthode qui permet à SPC d'envoyer des signaux au réseau de l'entrepreneur en ayant recours à une communauté BGP fournie par l'entrepreneur pour déclencher à distance un trou noir pour n'importe quel chemin Internet ou du réseau du Canada à titre de contremesure défensive dans le cas d'une attaque sur une partie du réseau du Canada, comme indiqué dans les documents RFC 3882 et 5635.

2.3 Configuration du PIS

- (57) Le PIS du SII doit être configuré pour le mode de détection automatique de duplex intégral.
- (58) L'entrepreneur devra fournir à partir de ses sources d'adresses une adresse IPv4 /30 statique et une adresse IPv6 /126 statique pour l'interconnexion entre son routeur interzones et le routeur interzones du réseau du Canada, et il devra désactiver tous les protocoles de configuration automatique sans état d'IPv6, de même que les protocoles DHCP et DHCPv6 depuis l'interface. Aucune adresse locale d'emplacement Ipv6 ne doit être utilisée. Les trames Ethernet acheminées sur

l'interface doivent comporter les types suivants : 0x0800 (IPv4), 0x0806 (ARP) et 0x86dd (IPv6).

- (59) Le service de l'entrepreneur doit prendre en charge le trafic IP pour des protocoles locaux de liaison, notamment IRDP, les réacheminements de protocole ICMP, les diffusions de protocole de routage intérieur (OSPF, IS-IS, IGRP, EIGRP), les protocoles de découverte appartenant au fournisseur (comme CDP et EDP), BOOTP, MPD, LLDP, et le protocole IEEE 802.1D ne doit pas être acheminé, sauf pour ARP, MLDv2 (document RFC 3810), IGMPv2 (document RFC 2236) 7 v3 (document RFC 3376) et le protocole de découverte de voisins IPv6 (document RFC 4861).

2.4 Soutien pour la diffusion groupée d'IPv4 et d'IPv6

- (60) Pour la diffusion groupée d'IPv4, l'entrepreneur doit :
- (60.a) établir une connexion en mode « sparse » de la version 2 du protocole PIM (document RFC 4601) à l'aide du routeur interzone du Canada.
 - (60.b) appliquer une limite PIM sur l'interface du routeur du fournisseur afin de définir ses propres domaines PIM, distincts du domaine PIM du Canada.
 - (60.c) établir un protocole homologue MSDP avec l'adresse IPv4 fournie au routeur interzones du Canada qui filtre les adresses de diffusion groupée indésirables en directions de sortie et d'entrée, selon les pratiques exemplaires actuelles, et qui accepte les paires de source (S, G) provenant du routeur interzones du Canada.
- (61) Pour IPv6, l'entrepreneur doit activer le mode « sparse » de la version 2 du protocole PIM dans l'interface de son routeur.
- (62) Pour l'interface se connectant au routeur interzone du Canada et le routeur de l'entrepreneur :
- (62.a) Pour la diffusion groupée d'IPv4, la version 2 du protocole IGMP ou une version plus récente (document RFC 3376) doit être activée dans l'interface.
 - (62.b) Pour la diffusion groupée d'IPv6, le protocole MLDv2 (document RFC 3810) doit être activé dans l'interface.
- (63) L'entrepreneur ne doit pas filtrer la diffusion groupée spécifique à la source du protocole PIM (documents RFC 3659 et 4608) pour la diffusion groupée d'IPv4 ou d'IPv6.
- (64) L'entrepreneur ne doit pas activer le mode « dense » du protocole PIM (document RFC 3973) dans l'interface connectée au routeur interzone du Canada.

2.5 Bande passante supplémentaire requise dans des situations particulières

- (65) L'entrepreneur doit en tout temps pouvoir prendre en charge le trafic IP supplémentaire au débit convenu, y compris les augmentations importantes et soudaines comparativement aux niveaux enregistrés le mois précédent. En cas de panne majeure de la configuration de l'interconnexion prévue, la totalité, et non juste une partie, du trafic IP sera acheminée vers Internet ou proviendra d'Internet et sera redirigée automatiquement vers le SII de l'entrepreneur.
- (66) L'entrepreneur doit fournir un débit supplémentaire pour répondre aux augmentations subites de trafic IP, permettre une croissance continue sans contraindre la demande et assurer la disponibilité constante du service Internet, puisqu'il ne sera pas avisé à l'avance de telles situations.

- (67) L'entrepreneur n'est pas autorisé à utiliser des circuits de débit minimal garanti ou de débit binaire non spécifié.
- (68) L'entrepreneur doit s'engager à réserver une bande passante.
- (69) L'entrepreneur peut utiliser des circuits configurés selon le principe du débit soutenu, du débit garanti, du débit à accès garanti ou de formes de débits similaires pour assurer la bande passante.
- (70) Le SII de l'entrepreneur doit avoir recours à un fonctionnement en duplex intégral.

2.6 Service de nettoyage anti-déni de service distribué

- (71) L'entrepreneur doit fournir sur demande dans son infrastructure un service de nettoyage anti-déni de service distribué.
- (72) L'entrepreneur doit offrir la possibilité d'analyser le trafic IP provenant d'Internet ou acheminé vers le réseau Internet, et de détecter et de supprimer (c.-à-d. nettoyer) le trafic IP malveillant selon les signatures, la réputation et les anomalies du trafic IP. L'entrepreneur doit permettre à SPC d'obtenir et d'exporter des métadonnées et des journaux associés à une cyber-attaque réelle ou présumée.
- (73) L'entrepreneur doit permettre au trafic IP légitime de se rendre à destination et empêcher toute attaque par déni de service susceptible de submerger le PIS du SII.
- (74) L'entrepreneur doit fournir l'accès au service de nettoyage anti-déni de service distribué et être en mesure de configurer son service à l'aide de l'OEIE.
- (75) L'entrepreneur doit fournir à SPC un accès sécurisé à l'OEIE.
- (76) L'entrepreneur doit permettre à SPC d'effectuer les activités suivantes dans l'OEIE :
 - (76.a) Exécuter, afficher et télécharger des rapports.
 - (76.b) Configurer et définir des rapports sur l'anti-déni de service distribué au besoin.
 - (76.c) Activer ou désactiver les mesures d'atténuation des attaques de déni de service distribué.
- (77) L'entrepreneur doit transmettre à SPC des alertes presque en temps réel, par courriel ou message texte, selon les événements d'intrusion ou les éléments déclencheurs configurés.
- (78) L'entrepreneur doit envoyer un courriel ou un message texte au début et à la fin de chacun des événements. Le message doit contenir des renseignements concernant le type d'événement, le service touché, le niveau de gravité, l'heure de début, l'heure de fin, les sources et les cibles de l'attaque de même que la description des conséquences.
- (79) L'entrepreneur doit communiquer en temps réel les données sur le trafic IP lié au déni de service distribué dans l'OEIE.
- (80) L'entrepreneur doit conserver les données cumulatives sur le trafic IP enregistrées aux 5 minutes au cours des 14 derniers jours et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (81) L'entrepreneur doit conserver les données cumulatives sur le trafic IP enregistrées aux 30 minutes au cours des 8 dernières semaines et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (82) L'entrepreneur doit conserver les données cumulatives sur le trafic IP enregistrées aux deux (2) heures au cours des six (6) derniers mois et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (83) L'entrepreneur doit conserver les données cumulatives sur le trafic IP enregistrées quotidiennement au cours des trois (3) dernières années et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (84) L'entrepreneur doit être proactif en demeurant à l'affût des cyber-menaces associées aux attaques de déni de service et transmettre à SPC des avis accompagnés de recommandations d'atténuation dès qu'il est informé de cyber-menaces visant SPC qui peuvent potentiellement avoir des répercussions sur le réseau du Canada. Il doit également appliquer les mesures d'atténuation nécessaires, une fois qu'elles ont été approuvées par SPC.

- (85) L'entrepreneur doit fournir des systèmes de nettoyage anti-déni de service distribué avec une capacité de protection initiale de 2 Gbps de bande passante sur Internet, avec la possibilité d'augmenter cette capacité sur demande par incréments de 1 Gbps.
- (86) L'entrepreneur doit être en mesure d'atténuer jusqu'à cinq (5) risques d'attaque continus, y compris les risques de trou noir, avec la possibilité d'augmenter ce nombre selon la demande.
- (87) L'entrepreneur doit prendre en charge une (1) configuration avec un profil de bande passante qui peut être appliquée globalement à tout le trafic au niveau du canal de communication du SII, ainsi que de multiples configurations et profils de bande passante pour les différents réseaux utilisant ce même canal.
- (88) L'entrepreneur doit fournir un système de nettoyage anti-déni de service distribué capable de reconnaître les tendances habituelles du trafic pour tous les profils, et ce, pendant des durées de normalisation spécifiques d'au moins soixante (60) jours, et pouvoir fixer des seuils normaux de bande passante en conséquence.
- (89) L'entrepreneur doit formuler des recommandations concernant la configuration initiale du système et fournir les seuils relatifs au réglage initial en guise de référence, et chaque fois que des mises à jour sont requises pendant toute la durée du contrat, à la demande de SPC et avec son approbation.
- (90) L'entrepreneur doit fournir ces mises à jour recommandées dans les 72 heures suivant l'incident, dans le cadre du rapport après incident, lorsqu'un incident de déni de service distribué n'est pas totalement atténué par le service offert et que des modifications doivent être apportées à la configuration et aux seuils du système. L'entrepreneur doit démontrer que ces recommandations sont formulées dans le meilleur intérêt de SPC.
- (91) L'entrepreneur doit répondre aux demandes de SPC si ce dernier l'avise d'une cybermenace imminente. Une fois la menace ciblée, l'entrepreneur doit prendre des mesures immédiates, conformément à la section 5.4, Gestion des incidents, afin de mettre en application les recommandations visant à offrir une protection contre les cybermenaces en modifiant la configuration et les seuils du système et en consignait le tout dans les rapports après incident aux fins de protection et de diligence raisonnable contre de futurs scénarios de cybermenaces potentiels.
- (92) L'entrepreneur doit fournir à SPC les coordonnées d'une personne-ressource qui répondra aux questions, discutera des cybermenaces et formulera des recommandations en vue d'atténuer les risques associés à un incident lié à la sécurité.

3 PRÉPARATION OPÉRATIONNELLE

3.1 Plan de préparation opérationnelle

- (93) Dans les quinze (15) JOGF suivant l'attribution du contrat, l'entrepreneur doit soumettre à l'approbation de SPC un plan de préparation opérationnelle (PPO) qui propose un calendrier de l'atteinte de l'état de préparation opérationnelle après l'attribution du contrat.
- (94) L'entrepreneur doit fournir un PPO révisé dans les cinq (5) JOGF suivant la réception des commentaires de SPC concernant le PPO.
- (95) Sauf indication contraire dans le présent document, l'entrepreneur doit réaliser le travail suivant (précisé dans les sections 3.2 à 3.5) dans les trente (30) JOGF suivant l'acceptation du PPO, à l'exception des jours dont SPC a besoin pour examiner et approuver le travail :
 - a) Plan de gestion du service;

- b) Plan de continuité du service;
 - c) Conception du service;
 - d) Description du service.
- (96) L'entrepreneur doit présenter à SPC un rapport d'étape hebdomadaire sur la préparation opérationnelle, lequel indiquera les renseignements suivants pour chaque tâche, jalon ou produit livrable qui figure dans le PPO :
- a) l'état actuel;
 - b) la date d'achèvement prévue;
 - c) le sommaire des travaux prévus pour la semaine qui fera l'objet du rapport suivant.
- (97) SPC organisera et dirigera une réunion de lancement du contrat dans les dix (10) JOGF suivant l'attribution du contrat. L'ordre du jour de la réunion sera défini par SPC puis transmis à l'entrepreneur avant la réunion de lancement du contrat.

3.2 Plan de gestion du service

- (98) L'entrepreneur doit fournir à SPC un plan de gestion du service qui comprend les éléments suivants :
- (98.a) une description sommaire du SII;
 - (98.b) un plan des ressources précisant la méthode à suivre pour déterminer les niveaux de ressources nécessaires à la réalisation des travaux indiqués dans le contrat;
 - (98.c) un plan d'assurance de la qualité précisant l'approche à suivre pour formuler et appliquer des normes relatives aux travaux et à la qualité, assurer la conformité avec les niveaux de service et passer en revue les travaux en cours;
 - (98.d) un plan de communication précisant l'approche à suivre afin de communiquer les exigences relatives à chacune des tâches, de résoudre les problèmes et les risques auxquels peuvent être confrontés l'entrepreneur et SPC, et de gérer les communications entre ces derniers;
 - (98.e) un plan organisationnel précisant la structure de gestion, les organisations, ainsi que les rôles et responsabilités des membres clés du personnel et des experts en la matière;
 - (98.f) un plan de gestion des risques précisant l'approche à suivre afin de relever les risques et d'en faire le suivi, d'isoler les déclencheurs d'événements associés aux risques, d'évaluer les probabilités et les incidences des risques, et d'élaborer un plan d'atténuation;
 - (98.g) un plan de gestion des problèmes précisant l'approche à suivre afin de relever et de gérer les problèmes de gestion du service, d'isoler les problèmes, d'en évaluer les incidences, de cerner les parties responsables, de mesurer la gravité des problèmes et d'établir les priorités et les processus en vue de déterminer une solution;
 - (98.h) un aperçu des systèmes d'information comprenant une description des systèmes qui seront mis en œuvre pour le SII.

3.3 Plan de continuité du service

- (99) L'entrepreneur doit présenter à SPC un plan de continuité du service qui vise à assurer la reprise du SII et des activités après sinistre et qui comprend les éléments suivants :
- a) une stratégie de rétablissement du service;

- b) les processus qui seront appliqués pour assurer la continuité du service (par exemple la stratégie de communication et l'établissement des priorités à l'égard du rétablissement du service);
- c) le transfert des fonctions de gestion et des opérations du centre des opérations principal au centre de relève;
- d) les stratégies de sauvegarde pour les installations, les données et systèmes de soutien opérationnel, et les principales composantes du service;
- e) l'assurance que les fournisseurs de l'entrepreneur (le cas échéant) ont mis en œuvre des plans et des stratégies de reprise après sinistre;
- f) les délais dans lesquels SPC peut s'attendre à ce que les services soient rétablis.

3.4 Conception du service

- (100) L'entrepreneur doit présenter à SPC une description de la conception du SII qui comprend les éléments suivants :
- a) la méthodologie de conception;
 - b) un plan de l'architecture de la sécurité du réseau pour le service offert, qui décrit la mise en œuvre de mesures de protection du périmètre de sécurité, le positionnement des services dans les zones de sécurité du réseau et les fonctions de redondance, d'extensibilité et de sécurité afin de répondre aux niveaux de service;
 - c) le contenu et le format des rapports et des documents;
 - d) les spécifications du fabricant pour l'ensemble du matériel qui sera déployé pour offrir le SII.

3.5 Description du service

- (101) L'entrepreneur doit présenter à SPC une description du SII qui comprend :
- a) un aperçu du SII;
 - b) les processus d'évaluation du niveau de service;
 - c) un aperçu des rapports de service à produire;
 - d) les processus de gestion du service (gestion des changements, des incidents, des problèmes, de la configuration, des versions, de la disponibilité et de la capacité);
 - e) les processus du bureau de service;
 - f) les processus du centre des opérations.

3.6 Évaluation de la sécurité et autorisation (ESA)

- (102) L'entrepreneur doit réaliser les travaux indiqués dans la présente sous-section conformément au processus d'évaluation de sécurité et d'autorisation de SPC pour le SII.
- (103) Le processus d'ESA doit être achevé avant la mise en œuvre du SII.
- (104) L'entrepreneur doit respecter les exigences en matière d'évaluation de sécurité et d'autorisation pour le SII, rassemblées en un processus à trois étapes :
- a) Étape 1 – Conception générale du service
 - i) Spécification générale de la sécurité de la conception du service

- ii) Matrice de traçabilité des exigences relatives à la sécurité (MTERS)
- b) Étape 2 – Conception détaillée du service
 - i) Spécification détaillée de la sécurité de la conception du service
 - ii) Matrice de traçabilité des exigences relatives à la sécurité
 - iii) Gestion des changements
 - iv) Protection de l'environnement de développement
 - v) Pratiques de développement sécurisées
 - vi) Procédures opérationnelles de sécurité
 - vii) Procédures d'installation des composants de sécurité
- c) Étape 3 – Installation
 - i) Plan d'essai et rapport d'essai sur la sécurité de l'intégration
 - ii) Plan et rapport d'évaluation et d'atténuation des vulnérabilités
 - iii) Plan et rapport de vérification de l'installation des composants de sécurité

3.6.1 Étape 1 – ESA de la conception générale du service

- (105) Dans les trente (30) JOGF suivant l'adjudication du contrat, l'entrepreneur doit soumettre à l'approbation de SPC une version provisoire des livrables suivants :
 - a) spécification générale de la sécurité de la conception du service (voir la sous-section Spécification générale de la sécurité de la conception du service);
 - b) matrice de traçabilité des exigences relatives à la sécurité (voir la sous-section Matrice de traçabilité des exigences relatives à la sécurité).
- (106) SPC examinera les livrables provisoires dans les cinq (5) JOGF.
- (107) Dans les cinq (5) JOGF suivant la réception des commentaires de SPC, l'entrepreneur doit lui remettre une version révisée des livrables.
- (108) SPC examinera les livrables révisés dans les cinq (5) JOGF.
- (109) Dans les deux (2) JOGF suivant la réception des commentaires de SPC, l'entrepreneur doit lui remettre la version finale des livrables.
- (110) L'entrepreneur doit attendre l'approbation de l'étape 1 par SPC avant de passer à l'étape suivante de l'évaluation de la sécurité et de l'autorisation.

3.6.1.1 Spécification générale de la sécurité de la conception du service

- (111) L'entrepreneur doit fournir à SPC un document de spécification de la sécurité de la conception du service qui décrit les aspects généraux du SII relatifs à la conception de la sécurité. Ce document doit contenir au moins les renseignements suivants :
 - a) un diagramme de haut niveau qui indique clairement la répartition des services et des composants entre les zones de sécurité du réseau et montre les principaux flux de données connexes à la sécurité;
 - b) la description des mesures de défense du périmètre des zones du réseau;
 - c) la description de l'utilisation des technologies de virtualisation, le cas échéant;
 - d) la description de la répartition de toutes les exigences techniques de sécurité parmi les éléments de conception générale du service dans toutes les couches architecturales;

- e) la description de la répartition de toutes les exigences non techniques de sécurité parmi les éléments organisationnels ou opérationnels de haut niveau;
 - f) la description de la méthode de gestion à distance;
 - g) la description de la méthode de contrôle d'accès;
 - h) la description de la méthode de gestion et de vérification de la sécurité;
 - i) la description de la méthode de gestion de la configuration;
 - j) la description de la méthode de gestion des correctifs;
 - k) la justification des principales décisions concernant la conception.
- (112) La spécification générale de la sécurité de la conception du service doit décrire la façon dont les concepts suivants seront mis en œuvre :
- a) contrôle d'accès;
 - b) gestion et vérification de la sécurité;
 - c) gestion de la configuration;
 - d) gestion des correctifs;
 - e) gestion à distance.
- (113) La spécification générale de la sécurité de la conception du service doit décrire la répartition des exigences de sécurité dans chacune des couches architecturales de la conception générale du service.
- (114) La spécification générale de la sécurité de la conception du service doit définir les couches architecturales (p. ex., couche communication, couche de virtualisation, couche de plateforme ou de SE, couche de gestion des données, couche d'intergiciels, couche d'application d'entreprise).
- (115) La spécification générale de la sécurité de la conception du service doit justifier explicitement les principales décisions connexes à la sécurité qui concernent :
- a) l'établissement de zones de sécurité du réseau;
 - b) les mesures de défense du périmètre du réseau et des zones du réseau;
 - c) l'utilisation des technologies de virtualisation.
- (116) La spécification générale de la sécurité de la conception du service doit être conforme à la conception du service (voir la sous-section Conception du service).

3.6.1.2 Matrice de traçabilité des exigences relatives à la sécurité

- (117) L'entrepreneur doit fournir à SPC une matrice de traçabilité des exigences relatives à la sécurité (MTERS) qui comprend les exigences de sécurité pour le SII, y compris des renvois à la documentation de spécification générale de la sécurité de la conception du service décrivant les mécanismes de sécurité à mettre en œuvre. La MTERS doit garantir que la spécification générale de la sécurité de la conception du SII satisfait pleinement aux exigences de sécurité du SII.
- (118) Tous les documents de service auxquels la MTERS renvoie doivent être fournis à SPC avec la matrice et décrire les mécanismes de sécurité avec suffisamment de précision pour permettre à SPC de s'assurer qu'ils satisfont pleinement aux exigences de sécurité du SII.
- (119) Pour chaque exigence de sécurité, la MTERS doit au moins fournir les renseignements suivants :
- (120) l'identifiant de l'exigence de sécurité qui relie l'exigence à l'énoncé correspondant de l'EDT (p. ex., l'identifiant de l'en-tête ou de la ligne);

- (121) le lien (la référence à un élément identifiable) avec des spécifications générales de conception du service.

3.6.2 Étape 2 – ESA de la conception détaillée du service

- (122) Dans les cinquante (50) JOGF suivant l'adjudication du contrat, l'entrepreneur doit soumettre à l'approbation de SPC une version provisoire de la spécification détaillée de la sécurité de la conception du service (voir la sous-section Spécification détaillée de la sécurité de la conception du service).
- (123) L'entrepreneur doit fournir une version à jour de la matrice de traçabilité des exigences relatives à la sécurité vers la conception détaillée du service (voir la sous-section Matrice de traçabilité des exigences relatives à la sécurité vers la conception détaillée du service).
- (124) SPC examinera les livrables provisoires dans les cinq (5) JOGF.
- (125) Dans les cinq (5) JOGF suivant la réception des commentaires de SPC, l'entrepreneur doit lui remettre une version révisée des livrables.
- (126) SPC examinera les livrables révisés dans les cinq (5) JOGF.
- (127) Dans les deux (2) JOGF suivant la réception des commentaires de SPC, l'entrepreneur doit lui remettre la version finale des livrables.
- (128) L'entrepreneur doit attendre l'approbation de l'étape 2 par SPC avant de passer à l'étape suivante de l'évaluation de la sécurité et de l'autorisation.

3.6.2.1 Spécification détaillée de la sécurité de la conception du service

- (129) L'entrepreneur doit fournir à SPC un document détaillé de spécification de la sécurité de la conception du service qui décrit les aspects détaillés du SII relatifs à la conception de sécurité. Ce document doit contenir au moins les renseignements suivants :
- un diagramme détaillé des composants (c'est-à-dire une version approfondie du diagramme de haut niveau);
 - la description de la répartition des mécanismes de sécurité techniques entre les éléments de conception détaillée du service;
 - la description de la répartition de tous les mécanismes de sécurité non techniques parmi les éléments organisationnels ou opérationnels de haut niveau;
 - la justification des principales décisions concernant la conception.
- (130) La spécification détaillée de la sécurité de la conception du service doit être conforme à la conception du service (voir la sous-section Conception du service) et à la spécification générale de la sécurité de la conception du service (voir la sous-section Spécification générale de la sécurité de la conception du service).

3.6.2.2 Matrice de traçabilité des exigences relatives à la sécurité vers la conception détaillée du service

- (131) L'entrepreneur doit fournir à SPC une matrice de traçabilité des exigences relatives à la sécurité (MTERS) qui comprend les exigences de sécurité pour le SII, y compris des renvois à la documentation de spécification détaillée de la sécurité de la conception du service décrivant les mécanismes de sécurité à mettre en œuvre. La MTERS doit garantir que la spécification détaillée de la sécurité de la conception du SII satisfait pleinement aux exigences de sécurité du SII.
- (132) Tous les documents de service auxquels la MTERS renvoie doivent être fournis à SPC avec la matrice et décrire les mécanismes de sécurité avec suffisamment de précision

pour permettre à SPC de s'assurer qu'ils satisfont pleinement aux exigences de sécurité du SII.

- (133) Pour chaque exigence de sécurité, la MTERS doit au moins fournir les renseignements suivants :
- a) l'identifiant de l'exigence de sécurité qui relie l'exigence à l'énoncé correspondant de l'EDT (p. ex., l'identifiant de l'en-tête ou de la ligne);
 - b) le lien (la référence à un élément identifiable) avec des spécifications générales de conception du service;
 - c) le lien (la référence à un élément identifiable) avec des spécifications détaillées de conception du service.

3.6.3 Étape 3 – Installation

3.6.3.1 Plan d'essai et rapport d'essai sur la sécurité de l'intégration

- (134) L'entrepreneur doit présenter à SPC un plan d'essai des mécanismes de sécurité qui documente les scénarios d'essai.
- (135) L'entrepreneur doit mettre en œuvre le plan d'essai des mécanismes de sécurité et présenter à SPC le rapport connexe qui décrit :
- a) les procédures d'essai afin de confirmer que les mécanismes sont mis en œuvre correctement et qu'ils respectent les normes applicables précisées dans les spécifications de la conception du service;
 - b) les résultats prévus et ceux obtenus pour chaque procédure d'essai des mécanismes de sécurité;
 - c) une description des mesures correctives apportées au SII pour chacun des écarts constatés par rapport aux résultats prévus ayant pu être corrigés au moment de la vérification;
 - d) l'inscription, dans le plan de traitement des risques, de chacun des écarts par rapport aux résultats prévus qui n'ont pu être corrigés au moment de la vérification (par exemple, parce que la correction aurait entraîné des modifications plus importantes).
- (136) L'entrepreneur doit permettre à SPC d'assister aux essais des mécanismes de sécurité, ce qui comprend :
- a) l'accès physique aux installations de l'entrepreneur hébergeant le SII;
 - b) la possibilité d'observer les représentants de l'entrepreneur pendant qu'ils exécutent les procédures d'essai des mécanismes de sécurité.

3.6.3.2 Plan et rapport d'évaluation et d'atténuation des vulnérabilités

- (137) L'entrepreneur doit permettre à SPC de réaliser une évaluation des vulnérabilités du SII, ce qui comprend :
- a) l'accès physique aux installations de l'entrepreneur où se trouve l'infrastructure du SII (composants matériels et logiciels);
 - b) l'accès réseau (ou les accès, s'il y a lieu) au SII afin de permettre l'analyse du réseau et des périphériques hôtes;
 - c) l'assistance d'au moins un membre du personnel qui connaît bien les aspects techniques du SII (c.-à-d. le matériel, les logiciels, les produits réseau et leur

configuration) tout au long de la partie de l'évaluation des vulnérabilités qui est effectuée sur place.

- (138) SPC peut réaliser une évaluation des vulnérabilités du SII et présenter à l'entrepreneur un rapport portant sur les vulnérabilités qu'il a détectées.
- (139) SPC limitera son évaluation à des activités de découverte et d'analyse et n'entreprendra pas d'activités perturbatrices ou destructives.
- (140) SPC peut aussi, à sa discrétion, exiger de l'entrepreneur qu'il effectue les essais liés à l'évaluation des vulnérabilités selon un plan que SPC a approuvé et qu'il lui présente les résultats.
- (141) L'entrepreneur doit présenter à SPC un rapport sur l'atténuation des vulnérabilités qui comprend :
 - a) une liste de vulnérabilités pour lesquelles SPC recommande la mise en œuvre de mesures correctives;
 - b) une description des mesures correctives à mettre en œuvre qui comprend les délais prévus;
 - c) la mise à jour de tous les documents touchés par les mesures correctives mises en œuvre, y compris les documents indiqués en référence dans la Matrice de traçabilité des exigences relatives à la sécurité.
- (142) L'entrepreneur doit exécuter les travaux qui permettront la production du rapport sur l'évaluation et l'atténuation des vulnérabilités, selon un plan approuvé par SPC.

3.6.3.3 Plan et rapport de vérification de l'installation des composants de sécurité

- (143) L'entrepreneur doit présenter à SPC un plan d'essai pour la vérification des mécanismes de sécurité qui documente les scénarios d'essai.
- (144) L'entrepreneur doit mettre en application le plan d'essai pour la vérification des mécanismes de sécurité et remettre à SPC un rapport sur la vérification de la sécurité.
- (145) Le rapport de vérification de la sécurité doit comprendre les éléments suivants :
 - a) les procédures de vérification employées afin de confirmer que les mécanismes de sécurité sont mis en œuvre correctement et respectent les normes applicables précisées dans les spécifications de la conception du service;
 - b) les résultats prévus et les résultats réels pour chaque procédure de vérification de la sécurité;
 - c) une description des mesures correctives apportées au SII pour chacun des écarts constatés par rapport aux résultats prévus ayant pu être corrigés au moment de la vérification;
 - d) l'inscription, dans le plan de traitement des risques, de chacun des écarts par rapport aux résultats prévus n'ayant pu être corrigés au moment de la vérification (p. ex., parce que la correction aurait entraîné des modifications plus importantes).
- (146) L'entrepreneur doit permettre à SPC d'assister aux essais portant sur la vérification des mécanismes de sécurité, ce qui comprend :
 - a) l'accès physique aux installations de l'entrepreneur hébergeant le SII;
 - b) la possibilité d'observer les représentants de l'entrepreneur pendant qu'ils exécutent les procédures de vérification des mécanismes de sécurité.

3.6.4 Concept des opérations de sécurité

- (147) L'entrepreneur doit présenter à SPC un rapport sur le concept des opérations de sécurité qui décrit les éléments suivants :
- a) la communauté des utilisateurs;
 - b) les applications de l'entrepreneur qui assurent le fonctionnement du service;
 - c) les centres de données et de communication de l'entrepreneur;
 - d) les rôles et responsabilités en matière de sécurité de l'entrepreneur;
 - e) l'analyse des incidents et les rapports suivant les incidents;
 - f) les contrôles d'accès;
 - g) l'environnement opérationnel de l'entrepreneur.

3.6.5 Plan de gestion des risques en matière de sécurité

- (148) L'entrepreneur doit présenter à SPC un plan de gestion des risques en matière de sécurité qui comprend :
- a) la façon dont les risques pour la sécurité seront signalés (à qui et à quelle fréquence);
 - b) les rôles et les responsabilités à l'égard de la gestion des risques en matière de sécurité;
 - c) la façon dont les risques pour la sécurité seront suivis et traités.

3.6.6 Architecture de sécurité

- (149) L'entrepreneur doit présenter à SPC un rapport sur l'architecture de sécurité qui décrit son infrastructure, c'est-à-dire :
- a) la façon dont les interfaces des zones d'accès public (décrites dans les publications ITSG-22 [<http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-fra.pdf>] et ITSG-38 [<http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-fra.pdf>] du Centre de la sécurité des télécommunications Canada [CSTC]) sont contrôlées de façon stricte, y compris tous les réseaux contrôlés externes comme Internet, dans un périmètre de sécurité défini;
 - b) la façon dont les autres zones de sécurité de réseau sont définies conformément au document ITSG-22 du CSTC;
 - c) la façon dont l'évaluation et l'autorisation de sécurité sont traitées conformément au document ITSG-33 en appui à la surveillance et à l'atténuation continues des risques, au moment de l'évaluation du rendement des contrôles de sécurité courants des systèmes de soutien à l'information;
 - d) l'équipement qu'utilise l'entrepreneur pour assurer la prestation du SII en interaction directe et indirecte avec l'infrastructure du gouvernement du Canada (p. ex., des routeurs) doit avoir été préalablement validé en vertu d'un système de critères communs reconnu, en le comparant à un profil de protection, ou en l'absence de ce dernier, à une cible de sécurité applicable dont les exigences en matière d'assurance sont conformes à la certification EAL-2 ou aux dispositions contenues dans une documentation approuvée en matière d'assurance;

- e) pour chiffrer les communications entre le gouvernement du Canada et l'entrepreneur, les modules cryptographiques servant à accéder à l'OEIE doivent être validés conformes à la norme FIPS 140-2 ou ultérieures;
- f) les modules cryptographiques validés conformes à la norme FIPS 140-2 doivent être configurés de façon à fonctionner en mode FIPS afin de n'utiliser que les algorithmes et les tailles de clés approuvés par le CSTC; les algorithmes et les tailles de clés approuvés par le CSTC sont décrits dans l'alerte de sécurité TI 11 version E (ITSA-11E) et peuvent être modifiés;
- g) l'entrepreneur doit inclure une brève description générale des diagrammes de réseau fournis.

3.6.7 Procédures opérationnelles de sécurité

- (150) L'entrepreneur doit présenter à SPC ses procédures opérationnelles de sécurité, lesquelles décrivent :
- a) les exigences de renforcement de système devant être appliquées aux serveurs, à l'entrepôt de données, aux périphériques réseau et aux applications, et les procédures de vérification utilisées;
 - b) les fonctionnalités de l'environnement opérationnel, dont :
 - i) la séquence de mise sous tension et de mise hors tension;
 - ii) l'utilisation de comptes systèmes privilégiés;
 - iii) la mise en marche et l'arrêt des systèmes (y compris le système d'exploitation et les applications);
 - iv) les communications de mise en marche et d'arrêt;
 - v) les opérations de sauvegarde et de restauration;
 - vi) les dérogations aux contrôles de sécurité (s'il y a lieu);
 - vii) la récupération et le redémarrage.
 - c) les priorités et les procédures liées aux interventions en cas d'incident visant l'atténuation des dommages, la limitation de la cause des incidents et le rétablissement des services, y compris l'envoi d'un avis à SPC;
 - d) les types d'événements ou d'activités qui constituent des incidents liés à la sécurité, la description des incidents liés à la sécurité informatique qui peuvent survenir, leurs répercussions possibles, les environnements technique et opérationnel et les priorités en matière de prestation de service;
 - e) un protocole concernant les violations de la confidentialité, qui comprendra, notamment, les processus de notification;
 - f) les processus de surveillance des vulnérabilités des systèmes en matière de sécurité et d'application des correctifs de sécurité au besoin.

3.6.8 Avis d'incident relatif à la sécurité

- (151) L'entrepreneur doit fournir des avis et générer des billets sur les incidents relatifs à la sécurité qui comprennent les renseignements suivants, sans toutefois s'y limiter :
- a) le genre et la description d'une attaque;

- b) la possibilité que l'attaque ait réussie, et ses répercussions;
- c) la portée de l'attaque (vise un seul groupe de clients ou de nombreux groupes);
- d) la source ou l'origine présumée de l'attaque, de l'incident ou de l'événement;
- e) les mesures prises;
- f) l'état de l'atténuation.

3.6.9 Plan de traitement des risques

- (152) L'entrepreneur doit présenter à SPC un plan de traitement des risques visant le suivi et le traitement de tous les éléments non résolus suivants :
 - a) les risques dans les cas où les exigences relatives à la sécurité ou les exigences fonctionnelles ne sont pas satisfaites;
 - b) les écarts notés lors des essais portant sur la vérification des mécanismes de sécurité et devant être corrigés;
 - c) les écarts notés lors des essais des mécanismes de sécurité et devant être corrigés;
 - d) les mesures correctives notées dans le rapport sur l'atténuation des vulnérabilités.
- (153) Pour chaque mesure corrective, le plan de traitement des risques doit comprendre les renseignements suivants :
 - a) la personne responsable de la mise en œuvre de la mesure corrective;
 - b) le délai visé pour l'atténuation des risques (date et version);
 - c) une évaluation du risque résiduel une fois la mesure corrective mise en œuvre;
 - d) le niveau de priorité établi par SPC, pour la mise en œuvre de chaque mesure corrective.

3.7 Mise en œuvre du SII

- (154) L'entrepreneur doit fournir les composants du SII et en assurer l'entretien.
- (155) L'entrepreneur doit mettre en œuvre le SII aux emplacements indiqués par SPC.
- (156) L'entrepreneur doit mettre en œuvre le SII conformément à ce qui suit et lors des mises à jour et des modifications successives des éléments :
 - a) la conception du service (voir la section Conception du service);
 - b) les exigences relatives à la sécurité;
 - c) l'architecture de sécurité (voir la section Architecture de sécurité);
 - d) les procédures opérationnelles de sécurité (voir la section Procédures opérationnelles de sécurité);
 - e) ITSB-60 : Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada (<http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb60-fra.html>);
 - f) ITSB-61 : Conseils sur l'utilisation du protocole de sécurité IP (IPsec) au sein du gouvernement du Canada (<http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb61-fra.html>);

g) Règles pour l'accessibilité des contenus Web 2.0 (WCAG 2.0) de W3C, niveau AA, directives 1 et 2 (<http://www.w3.org/TR/WCAG20/>);

- (157) L'entrepreneur doit mettre en œuvre les mesures correctives indiquées dans le rapport sur la vérification des mécanismes de sécurité, sur l'essai de ceux-ci et sur l'atténuation des vulnérabilités selon le plan de traitement des risques, en respectant l'ordre de priorité déterminé par SPC.
- (158) L'entrepreneur doit fournir, dans les vingt (20) JOGF suivant l'achèvement du plan de traitement des risques, un rapport qui présente les résultats des essais afin de vérifier l'efficacité des mesures correctives mises en œuvre.

3.7.1 Réunions et rapports sur l'état d'avancement

- (159) L'entrepreneur doit présenter à SPC des rapports hebdomadaires sur l'état d'avancement de la mise en œuvre du SII.
- (160) L'entrepreneur doit assister aux réunions planifiées par SPC afin de s'assurer que l'avancement des travaux respecte le calendrier de mise en œuvre.

3.7.2 Jalons de la mise en œuvre

- (161) Le plan de mise en œuvre doit comprendre les trois (3) jalons suivants :
- (161.a) conception préliminaire;
- (161.b) conception critique;
- (161.c) examen de la préparation opérationnelle.

3.7.2.1 Conception préliminaire

- (162) L'entrepreneur doit planifier une visite du site avec SPC et effectuer cette visite pour relever et évaluer tous les renseignements nécessaires en vue de l'installation et de la mise en disponibilité du SII au centre de données du Canada.
- (163) Les détails comprennent la liaison technique entre le SII de l'entrepreneur et le réseau GCNet, ainsi que les exigences de l'entrepreneur en ce qui a trait à l'alimentation électrique, à l'espace, au chauffage et à la ventilation.
- (164) L'entrepreneur doit documenter la visite du site et transmettre son rapport au Canada dans les deux (2) JOGF suivant la visite.
- (165) La conception préliminaire est terminée lorsque SPC approuve la visite du site.

3.7.2.2 Conception critique

- (166) L'entrepreneur doit présenter à SPC un document de configuration provisoire pour le SII à des fins d'examen. La version provisoire doit comprendre une copie de la configuration du routeur du SII de l'entrepreneur (les mots de passe doivent être supprimés de l'interface).
- (167) L'entrepreneur doit indiquer à SPC, à la suite de sa visite préparatoire, tout élément d'infrastructure manquant ou tout élément préalable que SPC pourrait devoir fournir en vue d'installations à venir.
- (168) L'entrepreneur doit fournir des renseignements sur le réseau et sur le service afin de démontrer que le SII qu'il fournit respecte toutes les exigences en matière de rendement.
- (169) L'entrepreneur doit indiquer si les renseignements fournis sont considérés comme exclusifs.

- (170) Après la réception du document de configuration du SII, l'entrepreneur doit rencontrer SPC pour discuter de tout problème décelé dans le document.
- (171) En fonction des commentaires formulés par SPC, l'entrepreneur doit soumettre à son approbation une version finale du document de configuration du SII.
- (172) Tout au long du contrat, l'entrepreneur doit assurer la tenue à jour du document de configuration du SII pour veiller à ce qu'il soit à jour et reflète la configuration réseau réelle du service.
- (173) L'entrepreneur doit présenter toute modification du document et obtenir l'approbation de SPC pour ces modifications dans les cinq (5) JOGF.
- (174) L'entrepreneur doit achever la conception du SII, la configuration réseau, la mise en place de l'équipement et la préparation des installations nécessaires à l'offre du service.
- (175) L'entrepreneur doit présenter à SPC ses procédures relatives aux opérations et à la gestion du service à cette étape.
- (176) La conception critique est terminée lorsque SPC approuve le document de configuration du SII et que les activités connexes sont achevées.

3.7.2.3 Examen de la préparation opérationnelle

- (177) L'entrepreneur doit réaliser suffisamment d'essais avant d'offrir ses services à SPC. L'entrepreneur doit consigner et documenter tous les résultats des essais et les transmettre à SPC à des fins d'examen et d'approbation.
- (178) L'entrepreneur doit soumettre à l'approbation de SPC les versions finales des procédures de gestion des opérations et du service.
- (179) SPC peut effectuer certains essais afin de valider le bon fonctionnement de chacun des services fournis par l'entrepreneur et vérifier que les exigences en matière de rendement sont respectées.
- (180) L'entrepreneur doit faciliter la réalisation des essais et aider SPC à cette fin. La période d'essai se tiendra 48 heures après que l'entrepreneur aura indiqué que le service est opérationnel. Pendant cette période, SPC peut :
 - (180.a) utiliser les commandes « ping » et « traceroute » ou toute autre procédure nécessaire pour tester la connectivité du réseau;
 - (180.b) vérifier que les numéros de réseau à transmettre à l'ensemble du réseau Internet sont transmis correctement;
 - (180.c) vérifier que les numéros de réseau qui ne doivent pas être transmis à l'ensemble du réseau Internet ne sont pas transmis;
 - (180.d) vérifier que les paquets non destinés au réseau GCNet ne passent pas par ce dernier pour se rendre d'une interface du SII à une autre;
 - (180.e) réaliser les tests nécessaires pour valider le rendement du SII comme la disponibilité, le débit de données, le délai de transit et la perte de paquets.
- (181) L'examen de la préparation opérationnelle est terminé une fois que SPC a approuvé tous les rapports, les documents et les procédures relatifs à l'OEIE énumérés dans la section de l'EDT portant sur la production de rapports et la documentation, et que le SII a réussi tous les essais d'acceptation et respecte les exigences en matière de rendement.
- (182) La réussite et l'approbation, par SPC, de l'examen de la préparation opérationnelle désignent le moment où l'entrepreneur peut commencer à facturer le SII.

3.7.3 Authentification, intégrité et confidentialité

- (183) Le SII doit être transparent afin de demander l'établissement d'un tunnel RPV à l'aide de l'un des services d'authentification suivants, selon les indications de SPC :
- a) Certificat
 - b) Serveur RADIUS
 - c) Serveur LDAP
 - d) Serveur SecurID
 - e) Active Directory
- (184) Le SII doit prendre en charge les certificats fournis par SPC.

3.7.4 Connectivité de réseau

- (185) L'entrepreneur ne doit pas mettre en place de pare-feu ou filtrer le trafic de protocole d'application.

4 GESTION DU SERVICE

- (186) L'entrepreneur doit avoir un gestionnaire du service qui agira à titre de personne-ressource et d'agent de liaison initial pour SPC concernant, entre autres :
- a) la transmission des incidents aux paliers supérieurs;
 - b) l'analyse des causes fondamentales (ACF);
 - c) les niveaux de service;
 - d) les activités de mise en œuvre;
 - e) le calendrier de l'entretien et des versions;
 - f) la qualité du service;
 - g) l'assurance du service;
 - h) la consultation à l'égard du service;
 - i) la production de rapports sur le service;
 - j) le rendement et la disponibilité du service;
 - k) les processus liés au service.
- (187) L'entrepreneur doit fournir un architecte de service qui agira à titre d'unique personne-ressource pour SPC concernant :
- a) la planification, la conception et l'ingénierie;
 - b) l'analyse des exigences et des répercussions;
 - c) la détermination et la recommandation des changements.
- (188) Le gestionnaire du service doit être disponible afin de rencontrer les représentants de SPC, entre 8 h et 17 h (heure de l'Est (HNE)) les JOGF, dans les deux (2) JOGF suivant une demande émise par SPC.
- (189) L'architecte de service doit être disponible afin de rencontrer les représentants de SPC, entre 8 h et 17 h (HNE) les JOGF, dans les deux (2) JOGF suivant une demande émise par SPC.

4.1 Centre des opérations

- (190) L'entrepreneur doit fournir un centre des opérations principal, en activité 24 heures sur 24, tous les jours de l'année, ayant l'infrastructure et les ressources nécessaires à la gestion et au fonctionnement centralisés du SII.
- (191) L'entrepreneur doit gérer et coordonner la mise en marche et l'arrêt de tous les composants sous sa responsabilité dans le cadre de la mise en disponibilité du SII sur demande, sans frais supplémentaires pour SPC. Cette tâche comprend les périodes durant lesquelles les centres de données gérés par SPC doivent être mis hors service, ce qui peut avoir des répercussions sur le fonctionnement des composants du SII hébergés au même emplacement.
- (192) L'entrepreneur doit également posséder un centre des opérations de relève, situé dans un endroit physique différent du centre principal (c.-à-d. dans un autre bâtiment), qui peut assumer toutes les fonctions opérationnelles et de gestion que prend en charge le centre principal.
- (193) Toute transition entre le centre principal et le centre de relève doit être transparente et ne doit avoir aucune incidence sur la disponibilité du SII.
- (194) L'entrepreneur doit assurer la transition entre le centre principal et le centre de relève selon le plan de continuité du service.
- (195) SPC se réserve le droit d'effectuer, à tout moment, des vérifications, dont certaines ponctuelles, portant sur les opérations et la gestion du service de l'entrepreneur afin de s'assurer du respect du présent contrat.

4.2 Continuité du service

- (196) L'entrepreneur doit mettre en œuvre le plan de continuité du service (l'ensemble des processus, procédures, rôles et responsabilités) dans les soixante (60) JOGF suivant l'achèvement du PPO et l'acceptation du service par SPC et présenter les résultats d'essai à SPC dans les dix (10) JOGF au terme de la mise à l'essai du plan de continuité du service.
- (197) L'entrepreneur doit corriger tous les problèmes décelés au cours de la mise à l'essai du plan de continuité du service, lequel sera examiné par le responsable technique jusqu'à ce que leur résolution ait été convenue.
- (198) L'entrepreneur doit fournir à SPC dans les trente (30) JOGF suivant chaque date anniversaire du contrat, une mise à jour de son plan de continuité du service.

4.3 Bureau de service du SII de l'entrepreneur

- (199) L'entrepreneur doit fournir un bureau de service que SPC pourra joindre en tout temps (24 heures sur 24, tous les jours de l'année).
- (200) Le bureau de service doit accepter les courriels que SPC envoie à la boîte de réception indiquée par l'entrepreneur. Celle-ci doit être dotée d'une fonction de réponse automatique pour accuser réception du courriel.
- (201) Le bureau de service doit accuser réception des courriels provenant d'adresses de courriel autorisées par SPC dans les 15 minutes suivant leur réception, et ce, en tout temps (24 heures sur 24, tous les jours de l'année).
- (202) L'entrepreneur doit fournir les numéros de téléphone suivants et les services de réseau téléphonique commuté public (RTCP) correspondants pour le bureau de service :
 - a) le numéro ou les numéros sans frais pour l'Amérique du Nord;

- b) l'accès TTY/FAX/ATS (téléimprimeur, télécopieur, appareil de télécommunication pour malentendants);
 - c) le numéro local dans la région de la capitale nationale, si possible.
- (203) Le bureau de service doit répondre aux appels (directement et à l'aide de messages préenregistrés) dans la langue officielle de SPC (français ou anglais) choisie par l'appelant. Ce dernier doit d'abord entendre un message, en français et en anglais, qui lui permet de faire ce choix.
- (204) L'entrepreneur doit surveiller le service 24 heures sur 24, tous les jours de l'année, et signaler immédiatement à SPC tout problème ayant une incidence sur le service.
- (205) L'entrepreneur doit fournir du soutien 24 heures sur 24, tous les jours de l'année, pour répondre aux appels de SPC au sujet de problèmes ayant une incidence sur le service.
- (206) L'entrepreneur doit collaborer avec la personne-ressource, indiquée dans le bon de travail ou la demande de commande de service, et avec SPC afin de résoudre les incidents et les problèmes qui ont une incidence sur le service.
- (207) L'entrepreneur doit aviser SPC dans les 15 minutes qui suivent la découverte d'un problème ou le signalement d'un incident ayant une incidence sur le service.
- (208) L'entrepreneur doit être en mesure de suivre, de surveiller et de signaler tout problème ayant une incidence sur le service.
- (209) L'entrepreneur doit donner aux personnes autorisées désignées par SPC l'accès en lecture à son système de gestion des appels de dépannage afin de faciliter la communication et la mise à jour des renseignements sur les incidents et les problèmes touchant le service.
- (210) L'entrepreneur doit, par courriel ou par téléphone, faire part à SPC de l'avancement de la résolution des problèmes critiques qui ont une incidence sur le service, et ce, toutes les 30 minutes jusqu'à ce que le service soit rétabli.
- (211) L'entrepreneur doit assister à des réunions pour discuter des problèmes ayant une incidence sur la prestation des services et pour les résoudre.
- (212) Les experts techniques de l'entrepreneur doivent assister aux réunions au besoin.
- (213) L'entrepreneur doit indiquer à l'avance le nom de l'entreprise désignée et le nom de la personne qui se rendra sur place.

4.4 Fonctionnement et surveillance du service

- (214) SPC se réserve le droit d'effectuer, à tout moment, des vérifications, dont certaines ponctuelles, portant sur les opérations et la gestion du service de l'entrepreneur afin de s'assurer du respect du présent EDT.
- (215) L'entrepreneur doit planifier des installations, des mises à niveau et des activités de gestion du service nouvelles et supplémentaires, y compris les modifications de la configuration (nouvelle version ou entretien du SII), pour qu'elles aient lieu les dimanches, entre minuit et 6 h, heure locale. Des exceptions sont permises au cas par cas, sous réserve de l'approbation de SPC.
- (216) L'entrepreneur doit soumettre un avis et des renseignements sur le travail à SPC et obtenir son approbation dix (10) JOGF avant l'exécution des travaux.
- (217) L'entrepreneur doit coordonner les installations, les mises à niveau, ainsi que la configuration et les réparations du service nouvelles et supplémentaires de concert avec SPC.

- (217.a) Pour ce faire, il doit communiquer avec la personne-ressource : avant le début des travaux et avant d'avoir désigné le ou les techniciens qui effectueront les travaux;
- (217.b) afin de l'informer des retards dans la réalisation des travaux au moment où l'entrepreneur constate que ceux-ci demanderont plus de temps que la durée d'interruption prévue;
- (217.c) afin de confirmer la réalisation des travaux et le rétablissement du service;
- (217.d) afin de transmettre par courriel un avis au responsable technique décrivant les travaux et confirmant leur réalisation.
- (218) L'entrepreneur doit surveiller et signaler tous les incidents 24 heures sur 24, tous les jours de l'année concernant les services fournis à SPC.
- (219) L'entrepreneur doit fournir du soutien 24 heures sur 24, tous les jours de l'année, pour répondre aux appels de SPC au sujet de problèmes liés au service.
- (220) L'entrepreneur doit travailler en collaboration avec SPC et d'autres entrepreneurs du SII afin de résoudre les incidents et les problèmes.
- (221) L'entrepreneur doit aviser par courriel ou par téléphone SPC dans les 15 minutes suivant la détection de problèmes ou le signalement d'incidents en lien avec le service.
- (222) L'entrepreneur doit utiliser un système de gestion des appels de dépannage pour assurer le suivi, la surveillance et la production de rapports pour tous les incidents et les problèmes en lien avec le service.
- (223) L'entrepreneur doit donner à SPC l'accès en lecture à son système de gestion des appels de dépannage afin de faciliter la communication et la mise à jour des renseignements sur les incidents et les problèmes liés au service.
- (224) L'entrepreneur doit, par courriel ou par téléphone, faire part à SPC de l'avancement de la résolution des problèmes et des incidents liés au service, plus particulièrement ceux qui touchent la sécurité, et ce, toutes les 30 minutes jusqu'à ce que le service soit rétabli et que les incidents soient atténués.
- (225) L'entrepreneur doit assister à des réunions à des endroits déterminés par SPC, après avoir reçu un préavis de trois (3) jours, pour discuter des problèmes concernant le rendement des services et pour les résoudre. Les experts techniques de l'entrepreneur doivent assister aux réunions au besoin.
- (226) L'entrepreneur doit aussi fournir les détails de la configuration du routeur du SII (sans les mots de passe) à SPC sur papier et en format électronique chiffré dans les 24 heures suivant une modification apportée à la configuration du routeur.

4.5 Évaluation de la sécurité et autorisation

- (227) Tout au long du cycle de vie du SII, l'entrepreneur doit suivre :
 - d) un processus opérationnel et de maintenance parvenu à maturité qui permet les essais des mécanismes de sécurité, l'évaluation des vulnérabilités, la production de rapports d'évaluation des risques, ainsi que la gestion des changements et de la configuration afin de veiller au maintien de la posture de sécurité du SII;
 - e) un processus parvenu à maturité visant l'élimination sécuritaire des biens de TI sensibles ayant trait au SII.
- (228) L'entrepreneur accepte que SPC puisse vérifier en tout temps sa conformité aux exigences de sécurité incluses dans le contrat. SPC informera l'entrepreneur à l'avance de ses vérifications prévues.

- (229) À la demande de l'autorité contractante, l'entrepreneur doit donner à SPC l'accès complet à ses locaux, à son réseau et à toutes les données ou bases de données liées au contrat du SII, à toute heure convenable.
- (230) L'entrepreneur doit fournir le personnel nécessaire à la réalisation d'entrevues, de même que tous les renseignements requis pendant la vérification.
- (231) Si SPC décèle des lacunes de sécurité pendant une vérification, l'entrepreneur doit les corriger à ses propres frais dans les délais établis avec SPC.
- (232) Tout au long du cycle de vie du SII, l'entrepreneur doit :
- atténuer les risques de façon à les maintenir à niveau acceptable selon SPC;
 - établir et consigner des niveaux d'acceptation des risques fondés sur des critères de risque conformément aux délais fixés par SPC pour la résolution des problèmes;
 - procéder à une évaluation et à une autorisation de sécurité conformément au contrat;
 - faire approuver ses opérations par SPC après toute modification à l'infrastructure du SII dont il assure le contrôle, de façon à pouvoir appliquer un programme d'inspection pour protéger la confidentialité, l'intégrité et la disponibilité des données de SPC contre les menaces et autres dangers. L'entrepreneur doit donner à SPC, sur demande et dans les 72 heures suivant cette demande, l'accès à ses installations du SII, à ses capacités techniques, à ses opérations, à ses documents, à ses dossiers, à ses bases de données, à ses journaux, à ses rapports et à ses résultats d'analyse. Cela comprend ses processus d'évaluation de la sécurité et d'autorisation, ainsi que de surveillance continue.
- (233) Le programme d'inspection doit comprendre, entre autres, les éléments suivants :
- des analyses visant à repérer les vulnérabilités des systèmes d'exploitation et des réseaux, authentifiés ou non;
 - des analyses visant à repérer les vulnérabilités des applications Web, authentifiées ou non;
 - des analyses visant à repérer les vulnérabilités des applications de base de données, authentifiées ou non.
- (234) L'entrepreneur accepte que le personnel ou des mandataires de SPC effectuent des analyses automatisées à l'aide de l'équipement exploité par SPC et des outils fournis par SPC à cet effet.

5 SERVICES DE GESTION

- (235) L'entrepreneur doit fournir tous les composants nécessaires à la prestation des services de gestion associés au SII, sans frais supplémentaires pour SPC.
- (236) L'entrepreneur doit fournir des services de gestion associés au SII sans frais supplémentaires pour SPC.
- (237) Afin d'administrer à distance les services de gestion associés au SII, l'entrepreneur doit suivre un processus approuvé par SPC et utiliser une connexion sécurisée (chiffrée) et fiable, qui comprend l'authentification forte des utilisateurs, la vérification de leur accès, la non-répudiation des changements et la protection de l'intégrité des données. L'entrepreneur doit mettre les journaux de vérification connexes à la disposition de SPC sur demande.

- (238) L'entrepreneur doit planifier les activités de gestion du service, y compris les modifications de la configuration (nouvelle version ou entretien du service), pour qu'elles aient lieu les dimanches, entre minuit et 6 h, heure locale. Des exceptions sont permises au cas par cas, sous réserve de l'approbation de SPC.
- (239) L'entrepreneur doit soumettre un avis à SPC et obtenir son approbation dix (10) JOGF avant l'exécution des travaux.
- (240) L'entrepreneur doit fournir les services de gestion suivants pour le SII, 24 heures sur 24, tous les jours :
- a) la gestion des commandes de service;
 - b) la gestion des changements;
 - c) la gestion de la configuration;
 - d) la gestion des incidents;
 - e) la gestion des versions;
 - f) la gestion de la capacité;
 - g) la gestion de la disponibilité.

5.1 Gestion des changements

- (241) L'entrepreneur doit créer une demande de changement et la transmettre à SPC pour tout changement à apporter au matériel, aux logiciels, aux applications ou aux processus qu'il utilise pour fournir le SII.
- (242) Toutes les demandes de changement doivent être approuvées par SPC.
- (243) Les changements à apporter à l'infrastructure du réseau et des systèmes de soutien de l'entrepreneur qui n'ont aucun lien avec la prestation du SII pour SPC n'ont pas à être approuvés par SPC.
- (244) L'entrepreneur doit créer au moins un dossier de changement par demande de changement présentée par SPC, dans un délai d'un (1) JOGF après la réception de la demande.
- (245) L'entrepreneur doit accepter les demandes de changement émanant de SPC 24 heures sur 24, tous les jours de l'année, au moyen d'une boîte de réception électronique dotée d'une fonction de réponse automatique qui accusera réception des demandes.
- (246) L'entrepreneur doit exécuter les demandes de changement non urgentes durant les périodes de maintenance approuvées par SPC.
- (247) L'entrepreneur doit transmettre les demandes de changement aux échelons supérieurs lorsque SPC l'exige.
- (248) Un dossier de changement doit au moins comprendre les champs d'information suivants propres aux demandes de changement, qui seront mis à jour par l'entrepreneur au besoin :
- a) le numéro du dossier;
 - b) la description du changement;
 - c) les dossiers de changement connexes;
 - d) le type;
 - e) l'état (ouvert, fermé, en cours, approuvé, en suspens, annulé, échoué, etc.);

- f) le numéro de dossier de changement de SPC;
 - g) l'information sur la personne-ressource de l'entrepreneur (nom, numéro de téléphone et adresse de courriel);
 - h) l'identificateur de l'organisation cliente;
 - i) les coordonnées de la personne-ressource de SPC (nom, numéro de téléphone et adresse de courriel);
 - j) le journal des activités;
 - k) la date et l'heure prévues du changement;
 - l) la date et l'heure d'achèvement du changement;
 - m) le nom de la personne qui a approuvé le changement;
 - n) les procédures de reprise.
- (249) À la demande de SPC, l'entrepreneur doit réviser le contenu des champs d'information de dossier de changement ou modifier le plan d'essai d'acceptation.
- (250) L'entrepreneur doit mettre à jour l'état du dossier de changement (échoué, réussi, etc.), conformément aux indications de SPC et en fonction de l'essai d'acceptation du changement et des résultats du retour en arrière (s'il y a lieu).
- (251) L'entrepreneur doit transmettre par courriel des renseignements sur les dossiers de changement associés aux demandes de changement précisées par SPC, en utilisant une liste de diffusion établie par SPC, jusqu'à ce que les dossiers soient fermés ou que SPC mette fin aux comptes rendus automatiques en fonction de l'état des dossiers de changement.
- (252) À la demande de SPC, l'entrepreneur doit annuler un changement en suivant les procédures de retour en arrière précisées dans le dossier de changement, qui comprennent :
- a) les tâches et activités nécessaires pour rétablir le service (fonctionnalités et données) à son état initial;
 - b) les résultats opérationnels attendus après l'annulation;
 - c) les critères permettant de vérifier si l'annulation est réussie;
 - d) la consignation des résultats de l'annulation dans le journal des activités du dossier de changement.
- (253) Lorsque les critères d'acceptation accompagnant la demande de changement ne sont pas respectés, l'entrepreneur doit annuler un changement en suivant les procédures de retour en arrière précisées dans le dossier de changement.
- (254) L'entrepreneur doit envoyer à SPC un avis d'exécution de demande de changement, au moins 48 heures avant l'exécution de la demande, une fois qu'il a évalué, approuvé et effectué tous les préparatifs nécessaires à cette mise en œuvre.
- (255) L'entrepreneur doit envoyer à SPC un avis d'annulation de demande de changement, au plus tard 24 heures après avoir annulé la demande.
- (256) L'entrepreneur doit procéder à un essai d'acceptation pour chaque changement, selon le plan indiqué dans le dossier de changement et approuvé par SPC, puis consigner les résultats de l'essai dans le journal des activités du dossier.

- (257) L'entrepreneur doit inscrire les résultats des essais d'acceptation dans le dossier de changement au plus tard deux (2) JOGF après l'achèvement d'une demande de changement.
- (258) L'entrepreneur doit mener à bien le plan d'essai d'acceptation figurant dans le dossier de changement avant que SPC accepte la demande de changement.
- (259) L'entrepreneur doit fermer le dossier de changement lié à une demande de changement une fois que celle-ci a été acceptée par SPC.
- (260) L'entrepreneur doit envoyer à SPC un avis d'achèvement de demande de changement, au plus tard deux (2) JOGF après l'achèvement de la demande.
- (261) L'entrepreneur doit permettre à SPC d'accéder aux dossiers de changement au moyen d'un navigateur Web qui permet :
 - a) d'obtenir une représentation hiérarchique des dossiers de changement et de consulter les renseignements d'un dossier (p. ex., les dossiers connexes) par zooms avant successifs;
 - b) de voir l'information sommaire au sujet des dossiers de changement ouverts ou fermés, présentée sous forme de tableau et de graphique, par année, mois, jour et heure, selon la période de son choix et pour un certain nombre de dossiers triés par type et état.

5.2 Gestion de la configuration

- (262) L'entrepreneur doit s'acquitter des tâches de gestion de la configuration suivantes pour le SII :
 - a) configurer et programmer toutes les fonctions, caractéristiques et modifications touchant les composants matériels et logiciels afin d'assurer en permanence le bon fonctionnement du SII, conformément aux exigences de SPC;
 - b) appliquer les correctifs matériels et logiciels;
 - c) tenir à jour l'information de configuration et l'état de tous les composants matériels et logiciels;
 - d) sauvegarder quotidiennement les fichiers de configuration (modifications apportées depuis la dernière version) et conserver les fichiers sauvegardés dans un emplacement différent;
 - e) tenir des fichiers journaux de configuration en y ajoutant, pour chaque changement de configuration, une entrée qui indique :
 - i) la date et l'heure du changement de configuration;
 - ii) la personne ayant apporté le changement de configuration;
 - f) fournir l'information de configuration des composants matériels et logiciels, au plus tard cinq (5) JOGF après que SPC en fait la demande, en respectant la convention d'appellation de fichier précisée par SPC et en utilisant un format de fichier commercial approuvé par ce dernier;
 - g) conserver la version actuelle et les versions précédentes de l'information de configuration;
 - h) faire le suivi des changements d'état (par exemple en conception, mise à l'essai, opérationnel ou retiré) d'un élément de configuration.

5.3 Gestion des incidents

- (263) L'entrepreneur doit collaborer avec SPC, ou toute tierce partie désignée par ce dernier, en vue de traiter les incidents et les problèmes rapidement et efficacement, tant pour la réponse que pour la résolution.
- (264) Avec l'aide de SPC, l'entrepreneur doit établir une communication directe avec les spécialistes et les techniciens de SPC et de l'entrepreneur dans le but de réduire au minimum les activités de résolution par le diagnostic et la localisation des incidents visant à déterminer leur cause fondamentale et une solution de rechange acceptable.
- (265) L'entrepreneur doit transmettre aux échelons supérieurs tout incident non réglé, sur la base d'échelons, de procédures et de processus clairs et bien établis.
- (266) L'entrepreneur doit fournir à SPC une matrice des échelons de transmission opérationnels et administratifs dans les cinq (5) JOGF suivant l'envoi d'une demande par SPC. Cette matrice contiendra la liste du personnel, ainsi que des suppléants (de même niveau hiérarchique) pour au moins cinq échelons supérieurs (du 1er au 5e échelon, le 5e échelon étant le niveau hiérarchique le plus élevé) et fournira des instructions claires sur la procédure de communication.
- (267) L'entrepreneur doit fournir à SPC les notifications d'incident selon les matrices de gestion et d'opération relatives à l'acheminement.
- (268) L'entrepreneur doit changer l'échelon de transmission propre à un incident dans les 15 minutes suivant une demande de SPC.
- (269) L'entrepreneur doit créer un dossier d'incident pour chaque incident.
- (270) L'entrepreneur doit consigner sous forme d'incidents les atteintes à la confidentialité ou à la sécurité de même que tout autre événement lié à la sécurité.
- (271) L'entrepreneur doit transmettre automatiquement par courriel des renseignements sur les dossiers d'incident sélectionnés par SPC, en utilisant une liste de diffusion établie par celui-ci, jusqu'à ce que les dossiers soient fermés ou que SPC mette fin à ces comptes rendus automatiques en raison du changement de l'état des dossiers.
- (272) Tout dossier d'incident doit comprendre à tout le moins les zones d'information suivantes, qui seront mises à jour par l'entrepreneur :
- a) le numéro du dossier;
 - b) la description de l'incident;
 - c) la personne ayant fait état de l'incident (entrepreneur ou représentant de SPC);
 - d) les dossiers d'incident connexes;
 - e) les dossiers de changement connexes;
 - f) la date et l'heure d'ouverture du dossier;
 - g) la date et l'heure de fermeture du dossier;
 - h) le type d'incident (production, essai fonctionnel, essai de rendement, sécurité, etc.) précisé par SPC;
 - i) la gravité de l'incident;
 - j) l'état de l'incident (ouvert, fermé, en cours, en suspens, annulé, etc.);
 - k) le numéro de dossier de SPC;
 - l) la fonction de service touchée;

- m) l'information sur la personne-ressource du bureau de service qui ouvre le dossier (nom, numéro de téléphone et adresse de courriel);
 - n) l'information sur la personne-ressource de l'entrepreneur (nom, numéro de téléphone et adresse de courriel);
 - o) l'identificateur de l'organisation cliente ou de l'utilisateur (précisé par SPC);
 - p) le type d'organisation cliente ou d'utilisateur (précisé par SPC);
 - q) la langue de l'organisation cliente ou de l'utilisateur;
 - r) l'information sur la personne-ressource du ministère (nom, numéro de téléphone et adresse de courriel).
- (273) Lorsque l'entrepreneur détecte un incident ou que SPC en signale un, l'entrepreneur doit ouvrir un dossier d'incident dans les cinq minutes suivantes.
- (274) L'entrepreneur doit mettre à jour le journal d'information sur les dossiers d'incident à la suite d'un changement d'état.
- (275) L'entrepreneur doit consigner toutes les transmissions d'incident aux échelons techniques ou administratifs supérieurs dans le journal d'information sur les dossiers d'incident.
- (276) L'entrepreneur doit aviser SPC par téléphone et par courriel dans les 15 minutes suivant la détection (24 heures sur 24, tous les jours de l'année) d'un incident de sécurité réel ou présumé, qu'il s'agisse d'un accès non autorisé, d'une attaque par déni de service, d'une fraude ou de toute autre atteinte à la sécurité.
- (277) L'entrepreneur doit faire le suivi de la durée d'interruption liée à chaque incident et l'inscrire dans les dossiers d'incident correspondants.
- (278) La durée d'interruption liée à un incident est calculée à partir du moment où celui-ci est détecté par l'entrepreneur ou signalé à l'entrepreneur par SPC.
- (279) La durée d'interruption liée à un incident se termine lorsque le SII est entièrement rétabli et que SPC a approuvé la fermeture des dossiers d'incident correspondants.
- (280) L'entrepreneur doit suspendre un incident (c'est-à-dire interrompre le chronométrage de l'interruption) à la demande de SPC.
- (281) Un incident suspendu par SPC doit demeurer suspendu jusqu'à ce qu'il soit relancé par SPC ou pour une période prédéterminée par SPC.
- (282) L'entrepreneur ne doit pas suspendre un incident sans l'autorisation de SPC, sauf s'il a demandé à celui-ci les renseignements nécessaires à la résolution de l'incident, mais que le responsable a été incapable de les lui fournir.
- (283) L'entrepreneur doit réactiver un incident qu'il a lui-même suspendu (c'est-à-dire reprendre le chronométrage de l'interruption) dès que SPC lui transmet les renseignements demandés.
- (284) L'entrepreneur doit suspendre le chronométrage de l'interruption si SPC en fait la demande ou si l'entrepreneur attend que SPC approuve une demande de fermeture de dossier d'incident, mais que celui-ci n'est pas disponible.
- (285) L'entrepreneur doit reprendre le chronométrage de l'interruption si SPC en fait la demande ou s'il est en mesure d'examiner la demande de fermeture de dossier et qu'il détermine que le dossier doit rester ouvert.
- (286) L'entrepreneur doit obtenir l'autorisation de SPC avant de fermer un dossier d'incident.

- (287) L'entrepreneur doit fermer les dossiers d'incident une fois que SPC en a autorisé la fermeture.
- (288) L'entrepreneur doit aviser SPC de la résolution d'un incident selon la gravité de celui-ci, tel que précisé par SPC.
- (289) Si un dossier d'incident est fermé et qu'un nouvel incident survient dans les 24 heures en raison du même problème, l'entrepreneur doit rouvrir le dossier initial, ou encore ouvrir un nouveau dossier qui renvoie au dossier initial et indiquer l'heure de début en fonction du premier incident.
- (290) L'entrepreneur doit déterminer et consigner les facteurs de causalité (causes fondamentales) de chaque incident.
- (291) L'entrepreneur doit élaborer des solutions de rechange pour toutes les causes fondamentales recensées.
- (292) L'entrepreneur doit qualifier de problème chronique tout incident qui se produit trois fois ou plus dans une période de 90 jours consécutifs et dont la cause fondamentale est la même.
- (293) L'entrepreneur doit hausser d'un niveau la gravité des incidents qualifiés de problèmes chroniques.
- (294) L'entrepreneur doit relier les incidents aux problèmes chroniques existants ou nouveaux, à la demande de SPC.
- (295) L'entrepreneur doit permettre à SPC d'accéder aux dossiers d'incident au moyen d'un navigateur Web qui permet :
- a) de rechercher et de trier des dossiers d'incident ouverts ou fermés par zone, période de référence (dates de début et de fin) et période (année, mois, semaine, jour ou heure) au choix de SPC;
 - b) de télécharger les résultats d'une recherche de dossiers d'incident selon la convention d'appellation de fichier précisée par SPC et dans un format de fichier commercial pour lequel il a donné son approbation;
 - c) d'obtenir une représentation hiérarchique des dossiers d'incident et de consulter les renseignements d'un dossier (p. ex., les dossiers connexes) par zooms avant successifs;
 - d) de voir l'information sommaire au sujet des dossiers d'incident ouverts ou fermés, présentée sous forme de tableau et de graphique, par année, mois, jour et heure, selon la période de son choix et pour un certain nombre de dossiers triés par type, gravité et état.

5.4 Gestion des versions

- (296) La gestion des versions doit :
- a) être intégrée aux processus de gestion des changements, des incidents et de la configuration;
 - b) comprendre la planification, la mise à l'essai et le déploiement des logiciels et du matériel modifiés ou nouveaux.
- (297) L'entrepreneur doit fournir des notes sur la version dans les quarante (40) JOGF précédant la mise en œuvre d'une nouvelle version du SII.
- (298) L'entrepreneur doit attendre l'approbation de SPC avant de mettre en œuvre une nouvelle version du SII.

- (299) À la demande de SPC, l'entrepreneur doit participer à des réunions de gestion des versions organisées par SPC afin de discuter des prochaines versions du SII.

5.5 Gestion de la capacité

- (300) L'entrepreneur doit s'acquitter des tâches de gestion de la capacité suivantes pour le SII :
- a) passer en revue et analyser les niveaux de service et les statistiques sur le rendement des services afin de détecter tout problème ou manque de capacité;
 - b) adapter, mettre au point et améliorer les services afin d'optimiser leur utilisation et leur rendement;
 - c) évaluer les besoins en matière de capacité du SII et formuler des recommandations quant aux changements de capacité des services.

5.6 Gestion de la disponibilité

- (301) Le SII de l'entrepreneur doit réagir à toute situation de panne de manière à maintenir la disponibilité de l'accès à Internet.
- (302) L'entrepreneur doit s'acquitter des tâches de gestion de la disponibilité suivantes :
- a) examiner les besoins en matière de disponibilité et s'assurer que des plans d'urgence sont établis et mis à l'essai périodiquement, conformément aux exigences de prestation de service;
 - b) cerner de façon proactive les problèmes de disponibilité afin de les régler avant qu'ils n'aient d'incidence sur le SII;
 - c) analyser les données sur la disponibilité en vue de détecter les problèmes à cet égard;
 - d) configurer les services afin d'assurer la disponibilité prévue au contrat.
- (303) Lors des réunions d'examen opérationnel hebdomadaires, l'entrepreneur doit signaler à SPC les problèmes susceptibles de réduire la disponibilité ou de provoquer un manque de capacité et proposer des solutions afin d'assurer la disponibilité prévue au contrat.
- (304) L'entrepreneur doit aviser SPC de toute interruption prévue du SII au moins vingt (20) JOGF à l'avance.
- (305) L'entrepreneur doit faire approuver toute interruption prévue du SII par SPC.

6 RÉUNIONS

- (306) Les réunions doivent se tenir en personne durant les heures de bureau (de 8 h à 17 h, HNE) des JOGF, à Ottawa en Ontario, sauf indication contraire de SPC.
- (307) SPC peut organiser une réunion trimestrielle de planification et d'examen du contrat. L'entrepreneur est tenu d'assister à cette réunion à la demande de SPC.
- (308) Durant les réunions de planification et d'examen du contrat, on peut examiner les points suivants liés aux travaux à accomplir :
- a) le rendement en matière de gestion du service du trimestre précédent;
 - b) les problèmes majeurs relativement à la prestation des services et au soutien, survenus au cours du trimestre précédent;
 - c) les améliorations importantes de la prestation des services et du soutien prévues pour le trimestre suivant;

- d) les risques, les possibilités et les objectifs propres au trimestre suivant.
- (309) L'entrepreneur doit organiser des réunions d'examen opérationnel et y participer par téléconférence ou d'autres moyens précisés par SPC. La fréquence de ces réunions sera convenue entre SPC et l'entrepreneur après l'attribution du contrat. Ces réunions auront lieu au moins une fois par mois ou plus fréquemment, selon le volume et la gravité des questions opérationnelles à traiter. Ces réunions visent à examiner les problèmes qui ont une incidence sur le service et le résultat des modifications apportées depuis la réunion précédente, à examiner les problèmes survenus depuis la dernière réunion, l'avancement des interventions en cours, ainsi que l'approbation et la planification des mesures correctives recommandées dans les rapports d'ACF.
- (310) L'entrepreneur doit organiser, à la demande de SPC, des réunions portant sur la gestion des changements et y participer par téléconférence ou d'autres moyens précisés par SPC. Ces réunions visent à examiner les résultats des demandes de changement exécutées la semaine précédente, les demandes de changement prévues pour la prochaine semaine et celles soumises à l'approbation de SPC par l'entrepreneur.
- (311) L'entrepreneur doit organiser tous les trois mois une réunion d'examen des niveaux de service et y participer par téléconférence ou d'autres moyens précisés par SPC. Cette réunion vise à déterminer si les niveaux de service ont été atteints durant les trois mois précédents. Avant la réunion, l'entrepreneur doit se préparer à discuter de tout manquement aux niveaux de service, à décrire les mesures prises afin d'empêcher que des situations néfastes pour les services ne se reproduisent et à examiner les plans d'évolution des services pour les trois prochains mois.
- (312) L'entrepreneur doit organiser des réunions hebdomadaires et y participer afin d'examiner les DCS nouvelles ou non réglées.
- (313) L'entrepreneur doit assurer la disponibilité de toutes les ressources pertinentes qui seront présentes aux réunions ou il doit pouvoir communiquer avec elles au cours des réunions, par téléconférence ou d'autres moyens.

7 RAPPORTS ET DOCUMENTATION

- (314) L'entrepreneur doit fournir tous les rapports et autres documents requis désignés dans l'EDT, y compris les documents énumérés et décrits dans la présente section.
- (315) L'entrepreneur doit fournir tous les rapports et autres documents concernant le SII en anglais, dans un format de fichier commercial approuvé par SPC.
- (316) L'entrepreneur doit publier les rapports sur son OEIE pour que les personnes autorisées désignées par SPC puissent y accéder et les télécharger.
- (317) L'entrepreneur doit assurer le suivi des versions et des modifications de tous les rapports et autres documents concernant le SII.
- (318) L'entrepreneur doit archiver les données de tous les rapports concernant le SII pendant la durée du contrat et transmettre à SPC les données demandées dans les vingt (20) JOGF suivant la réception d'une demande écrite de sa part, selon le format de fichier et la convention d'appellation de fichier précisés par SPC.
- (319) L'entrepreneur ne doit pas exiger l'utilisation de composants ActiveX pour l'accès aux rapports et aux autres documents concernant le SII.
- (320) Sauf indication contraire du présent EDT au sujet d'un rapport particulier, l'entrepreneur doit fournir chaque rapport mensuel cinq (5) JOGF après la fin du mois visé par le rapport.

- (321) L'entrepreneur doit maintenir l'exactitude des renseignements et fournir des documents à jour à SPC dans les cinq (5) JOGF après avoir effectué une modification ou une mise à jour.
- (322) L'entrepreneur doit mettre à jour tout document ou schéma concernant le SII à la suite d'un changement :
 - a) qui a une incidence sur l'information contenue dans le document ou le schéma relatif au SII, ou
 - b) que SPC exige avant d'accepter le document ou le schéma.
- (323) L'entrepreneur doit fournir des rapports d'examen rétrospectif qui renferment les leçons tirées de la résolution des problèmes survenus. Ces rapports doivent être publiés dans l'OEIE et demeurer accessibles pour la durée du contrat une fois archivés.
- (324) L'entrepreneur doit fournir des rapports d'inventaire par type de service et par emplacement, auxquels le responsable technique doit pouvoir accéder à partir de l'OEIE, conformément à la section 7.3, Document de configuration.

7.1 Rapports mensuels

- (325) L'entrepreneur doit envoyer à SPC un rapport mensuel sur l'état du contrat, qui contient :
 - a) les problèmes de niveau de service devant être résolus;
 - b) les risques, y compris leur probabilité et les mesures d'atténuation correspondantes;
 - c) les différends en matière de facturation devant être résolus.
- (326) L'entrepreneur doit envoyer à SPC un rapport mensuel sous forme de tableau et de graphique qui contient, pour chaque cas où un niveau de service n'a pas été atteint :
 - a) le niveau de service calculé;
 - b) le niveau de service prévu au contrat;
 - c) la description du non-respect du niveau de service;
 - d) les crédits de service applicables.
- (327) L'entrepreneur doit envoyer à SPC un rapport mensuel sur ses dépenses financières.

7.2 Rapports sur demande spéciale

- (328) L'entrepreneur peut être tenu de fournir à SPC un rapport spécial sur les atteintes à la sécurité, qui couvre la période de référence précisée par SPC et qui contient :
 - a) le nombre d'incidents de sécurité et de mesures prises;
 - b) le nombre d'enquêtes sur la sécurité effectuées;
 - c) les délais d'intervention moyen et maximal pour les incidents de sécurité;
 - d) les durées moyenne et maximale des enquêtes sur la sécurité.
- (329) L'entrepreneur peut être tenu de fournir des rapports spéciaux sur tous les incidents graves, qui contiennent les mesures de suivi des questions en suspens.

- (330) L'entrepreneur peut être tenu de fournir à SPC, sur demande spéciale, un rapport d'inventaire spécial décrivant l'équipement dont sont dotés les emplacements en ce qui concerne le SII, dans les dix (10) JOGF suivant la modification de l'information contenue dans le rapport précédent. Le rapport doit indiquer :
- a) l'équipement appartenant à l'entrepreneur;
 - b) le fabricant de l'équipement et son pays d'origine;
 - c) le modèle et le numéro de série de l'équipement;
 - d) la date d'installation de l'équipement;
 - e) la date de la dernière mise à jour du micrologiciel.
- (331) L'entrepreneur peut être tenu d'envoyer à SPC des rapports de gestion sur l'état des opérations, qui contiennent :
- a) un rapport sommaire sur l'ensemble du service;
 - b) une vue sous forme de tableau et de graphique qui couvre une période de 13 mois et qui indique :
 - i) la valeur cible, la valeur réelle et le nombre d'exceptions pour chaque niveau de service;
 - ii) le nombre de demandes de changement présentées, exécutées et échouées;
 - iii) les écarts minimal, maximal et moyen entre les durées prévues et réelles pour l'exécution des demandes de changement;
 - iv) le nombre d'incidents;
 - v) les durées minimale, maximale et moyenne d'ouverture et de fermeture des incidents par gravité et type;
 - c) un résumé des demandes de changement urgentes;
 - d) des renseignements sur les incidents et les demandes de changement pour lesquels le processus de transmission aux échelons supérieurs a échoué ou n'a pas été suivi;
 - e) les mesures correctives à prendre pour éviter le non-respect des niveaux de service à l'avenir et les délais de mise en œuvre des changements requis.
- (332) L'entrepreneur peut être tenu d'envoyer à SPC des rapports sur les problèmes chroniques, qui contiennent :
- a) la description des problèmes chroniques;
 - b) les mesures prises pour régler les problèmes chroniques;
 - c) des recommandations sur la façon d'éviter des problèmes chroniques semblables à l'avenir.
- (333) L'entrepreneur peut être tenu d'envoyer à SPC des rapports sur chaque niveau de service, qui comprennent :
- a) les données cumulatives quotidiennes sur le niveau de service pour les 60 derniers jours;
 - b) les données cumulatives quotidiennes sur le niveau de service pour les 13 derniers mois;

- c) les données cumulatives mensuelles sur le niveau de service depuis l'attribution du contrat.

7.3 Document sur la configuration

- (334) L'entrepreneur doit fournir un document sur la configuration du SII qui contient la description de la conception et de la configuration de l'équipement et des installations déployés par l'entrepreneur pour la prestation du SII.
- (335) Le document doit comprendre une représentation graphique de la portion du réseau de l'entrepreneur qui sert à fournir le service aux intranets de SPC, y compris chacun des routeurs, des nœuds et des interfaces vers les réseaux externes.
- (336) L'entrepreneur doit conserver et mettre à jour le document de configuration du SII pendant toute la durée du contrat. Toute modification apportée au document doit recevoir l'approbation de SPC.
- (337) Le document de configuration sur le SII doit au moins contenir les renseignements suivants :
- (337.a) une représentation graphique de la portion du réseau de l'entrepreneur qui sert à fournir le SII sur le réseau GCNet, y compris chacun des routeurs, des nœuds et des interfaces vers les réseaux externes, ainsi que les installations de communication utilisées pour les relier;
- (337.b) la capacité des installations de télécommunication, ainsi que les seuils de rendement pour satisfaire aux exigences en matière de haute disponibilité et de diversité;
- (337.c) la configuration de l'interface du routeur de l'entrepreneur pour le SII, sans les mots de passe;
- (337.d) la description de l'interconnexion Internet aux points d'accès au réseau, des échanges de réseaux urbains et des dispositions d'homologage de réseau (IPv4 et IPv6) accompagnées des adresses d'interface de l'entrepreneur;
- (337.e) un schéma fonctionnel illustrant la connectivité entre le réseau de l'entrepreneur et d'autres systèmes autonomes directement connectés, y compris des connexions entre systèmes autonomes qui ne sont pas établies à l'aide de la version 4 du protocole BGP;
- (337.f) une description des significations particulières propres à l'entrepreneur ou des fonctionnalités concernant les attributs du protocole BGP (p. ex., valeurs ou significations particulières de l'attribut « communauté »);
- (337.g) une description des moyens utilisés par l'entrepreneur pour réduire ou éliminer le flux des données de routage sur le réseau GCNet grâce à la sélection de l'information de routage transmise (c.-à-d. le filtrage des chemins parcourus ou des mécanismes similaires);
- (337.h) une description des moyens utilisés par l'entrepreneur pour instaurer des voies d'acheminement pour les numéros du réseau GCNet, notamment l'emplacement du registre de routage et la façon dont l'entrepreneur le tient à jour, la méthode utilisée par l'entrepreneur pour acheminer le trafic de transit IP sur le réseau GCNet, le filtrage (autre que les filtres de chemins parcourus) et les autres fonctionnalités propres à l'entrepreneur (p. ex., l'attribut RIPE « consultatif ») qui peuvent avoir une incidence sur le comportement de routage, ainsi qu'une description des procédures administratives utilisées pour informer le fournisseur de services en amont des modifications désirées.
- (338) L'entrepreneur doit veiller à l'exactitude des renseignements et mettre à jour les documents de configuration du SII qui s'y rapportent pour toute la durée du contrat.

- (339) L'entrepreneur doit fournir des documents à jour dans les cinq (5) JOGF concernant toute modification ou mise à jour.
- (340) Toute nouvelle version du document de configuration du SII doit être approuvée par SPC.

8 RAPPORTS DE GESTION

8.1 Outil d'échange d'information électronique (OEIE)

- (341) L'entrepreneur doit mettre à la disposition de SPC un outil d'échange d'information électronique (OEIE) ou un outil équivalent fiable et sécurisé, que le SPC doit approuver immédiatement après l'attribution du contrat.
- (342) L'entrepreneur doit permettre à SPC d'utiliser cet outil dans les 60 JOGF après l'attribution du contrat.
- (343) L'OEIE de l'entrepreneur doit être destiné à accueillir, entre autres, des rapports sur les niveaux de service, de la documentation technique et opérationnelle, les résultats des essais et des factures électroniques, ou à y accéder.
- (344) L'entrepreneur doit protéger la confidentialité de l'information publiée en permettant uniquement aux personnes autorisées désignées par SPC d'y accéder.
- (345) Si l'OEIE approuvé de l'entrepreneur est un portail Web ou une autre application équivalente :
 - (345.a) L'entrepreneur doit, sur demande, créer et gérer des comptes d'utilisateur pour les personnes désignées par SPC.
 - (345.b) L'OEIE doit consigner automatiquement tous les accès et l'entrepreneur doit fournir les journaux d'accès à SPC à sa demande.
 - (345.c) Dans l'OEIE de l'entrepreneur, les mots de passe pour la connexion des utilisateurs doivent :
 - (345.c.1) être composés d'au moins six caractères;
 - (345.c.2) être modifiés tous les 60 jours;
 - (345.c.3) contenir des majuscules et des minuscules et au moins un chiffre.
 - (345.d) L'entrepreneur doit limiter l'accès à l'OEIE par adresses IP et numéros de port d'application.
 - (345.e) L'entrepreneur doit mettre en œuvre le protocole TLS (Transport Layer Security) dans son OEIE et chiffrer les sessions à l'aide de l'algorithme 3DES (3 Key Triple Data Encryption Standard) ou AES (Advance Encryption Standard).
- (346) L'entrepreneur doit protéger l'OEIE et l'information qu'il contient conformément aux pratiques exemplaires et aux normes de l'industrie, notamment par l'utilisation de systèmes de détection des intrusions, de logiciels antivirus, de pare-feu et de routeurs filtrant les adresses IP.
- (347) L'entrepreneur peut demander la permission de s'écarter de ces exigences ou proposer un périmètre de sécurité différent, sous réserve de l'approbation de SPC.
- (348) L'entrepreneur doit fournir un OEIE qui permet à SPC d'exécuter, d'afficher et de télécharger des rapports.
- (349) L'entrepreneur doit fournir des rapports, qui doivent être disponibles en formats HTML, XML et CSV ou dans d'autres formats approuvés par SPC.
- (350) L'entrepreneur doit veiller à ce que SPC soit en mesure de personnaliser les rapports en fonction du système d'information fourni.

- (351) L'entrepreneur doit offrir à SPC la possibilité d'activer ou de désactiver sur l'OEIE les mesures d'atténuation des attaques par déni de service.
- (352) L'entrepreneur doit publier sur son OEIE les mises à jour relatives à un changement proposé dans les cinq (5) JOGF suivant son approbation dans le cadre du processus de gestion des changements décrit à la section 5.2.

8.2 Données sur le trafic IP

- (353) L'entrepreneur doit communiquer en temps réel les données sur le trafic IP sur l'OEIE.
- (354) L'entrepreneur doit conserver les données cumulatives sur le trafic IP, ainsi que sur le trafic IPv4 et IPv6 distinct enregistrées aux 5 minutes au cours des 14 derniers jours et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (355) L'entrepreneur doit conserver les données cumulatives sur le trafic IP, ainsi que sur le trafic IPv4 et IPv6 distinct enregistrées aux 30 minutes au cours des huit dernières semaines et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (356) L'entrepreneur doit conserver les données cumulatives sur le trafic IP, ainsi que sur le trafic IPv4 et IPv6 distinct enregistrées aux deux (2) heures au cours des six (6) derniers mois et les rendre accessibles sur l'OEIE aux fins d'interrogation.
- (357) L'entrepreneur doit surveiller et enregistrer l'utilisation des données IP entrantes et sortantes à leurs PIS respectifs depuis le réseau GCNet aux cinq (5) minutes, 24 heures sur 24, tous les jours de l'année.

8.3 Rapports de lutte contre le déni de service

- (358) L'entrepreneur doit fournir des rapports sur les méthodes de lutte contre le déni de service distribué, lesquels :
 - (358.a) doivent être disponibles en formats HTML, XML et CSV ou dans d'autres formats approuvés par SPC;
 - (358.b) doivent être automatiquement envoyés, à intervalles réguliers, aux adresses de courriel fournies par SPC;
 - (358.c) doivent illustrer l'utilisation du trafic IP entrant et sortant sur le réseau pour les 100 applications les plus utilisées réparties par port d'application pour les protocoles TCP et UDP (p. ex., http, https, smtp), et fournir un sommaire du trafic IP par protocole IP;
 - (358.d) doivent indiquer les 100 adresses qui utilisent le plus de bande passante en tant que rapport sommaire Top Talker;
 - (358.e) doivent fournir des renseignements sur les vers informatiques et les hôtes contaminés du réseau sous forme de rapport d'activités des vers informatiques;
 - (358.f) doivent fournir des renseignements sur le nettoyage des données IP sur le trafic sous forme de rapport d'atténuation des menaces;
 - (358.g) doivent fournir des renseignements sur l'importance du trafic IP entrant, interrompu et autorisé.

8.4 Procédures de gestion des opérations

- (359) Les communications entre l'entrepreneur et SPC doivent être coordonnées et transmises par l'entremise du Canada.
- (360) L'entrepreneur doit transmettre les renseignements quotidiens de routine sur les opérations et la gestion du service au Centre des opérations de réseau et au bureau de

service de SPC et coordonner les activités connexes avec les personnes-ressources désignées et autorisées, une fois que les activités auront été officialisées par SPC.

(361) Les procédures de gestion des opérations de l'entrepreneur doivent décrire en détail à l'intention de SPC les processus et les procédures de l'entrepreneur relativement aux opérations et à la prestation du service.

(362) L'entrepreneur doit fournir à SPC les procédures de gestion des opérations telles qu'il est décrit dans les en-têtes de chacune des sous-sections suivantes :

8.4.1 Gestion des incidents et des problèmes

(362.a.1) Système de dossiers d'incident et processus connexes

(362.a.2) Organigramme de traitement des incidents

(362.a.3) Procédures de signalement des incidents et de transmission aux échelons supérieurs

(362.a.4) Délais de résolution

(362.a.5) Analyse des causes fondamentales

8.4.2 Centre de dépannage et organisation de soutien de l'entrepreneur

(362.a.6) Accès et soutien 24 heures sur 24, tous les jours de l'année

(362.a.7) Numéro de téléphone et adresse de courriel du centre d'assistance

8.4.3 Système et procédures de gestion des changements

(362.a.8) Traitement des types de changements (urgence, maintenance, version, etc.)

(362.a.9) Organigramme du processus de commande et d'approvisionnement

(362.a.10) Délais d'exécution

8.4.4 Procédures de gestion de la sécurité

(362.a.11) Politique de sécurité de l'entrepreneur

(362.a.12) Systèmes de contrôle de sécurité

(362.a.13) Attestations de sécurité du personnel, selon lesquelles chacun des employés de l'entrepreneur, et toute personne ou employé d'un sous-traitant de l'entrepreneur, qui contribuera à la prestation du service pour le Canada, y compris la gestion, l'administration et le soutien technique de ces composants, doit détenir une attestation de sécurité du personnel cotée SECRET et la nationalité canadienne.

8.5 Procédures de gestion du service

L'entrepreneur doit présenter à SPC les procédures de gestion du service qui décrivent en détail ses processus en la matière. Les procédures de gestion du service doivent comprendre :

(362.b) une liste des mesures du service pour chacun des services;

(362.c) la méthode et la fréquence des mesures du service;

(362.d) les calculs servant à déterminer les valeurs des niveaux de service qui sont communiquées;

(362.e) un sommaire des formats utilisés pour les rapports sur les niveaux de service;

(362.f) les objectifs et les garanties relatifs aux niveaux de service (s'il y a lieu) pour chacun des services.

8.6 Rapports sur les niveaux de service

(363) L'entrepreneur doit présenter à SPC les rapports mensuels exigés sur les niveaux de service, au plus tard le dixième jour du mois suivant le mois visé, aux fins d'examen et

d'approbation. Ces rapports contiennent des renseignements sur le rendement du service issus de la surveillance et des mesures.

- (364) L'entrepreneur doit publier les rapports sur les niveaux de service sur son OEIE. Les rapports doivent comprendre ce qui suit :
 - (364.a) les valeurs relatives au rendement du service de l'entrepreneur;
 - (364.b) un rapport sur les dossiers d'incident et les problèmes qui décrit les incidents, les problèmes, les diagnostics, les mesures correctives et les délais de résolution;
 - (364.c) un rapport sur le traitement des demandes qui indique la description, la date de début et la date de fin des demandes en cours et de celles qui sont terminées.
- (365) À la demande de SPC, l'entrepreneur doit lui présenter, dans les cinq (5) JOGF, un rapport d'ACF et un rapport sur les interruptions de la prestation du service décrivant les incidents, les diagnostics, les problèmes, les mesures correctives et les stratégies d'atténuation visant à empêcher que des incidents similaires se reproduisent.

8.7 Demandes de commande de service

- (366) L'entrepreneur doit permettre le traitement et le suivi des demandes de commande de service par l'intermédiaire de l'OEIE.

8.8 Document de contrôle d'interface (DCI)

- (367) L'entrepreneur doit fournir des DCI qui contiennent les renseignements sur le service relatifs à l'interface technique entre le SII de l'entrepreneur et les intranets de SPC.
- (368) SPC doit fournir à l'entrepreneur un modèle de DCI vierge suivant l'attribution du contrat. Une fois complété, le document doit contenir tous les renseignements requis par l'entrepreneur pour mettre en service et soutenir l'interface reliant son service aux intranets de SPC.
- (369) L'entrepreneur doit fournir les renseignements suivants dans son DCI :
 - (369.a) ses coordonnées;
 - (369.b) une description de la couche physique du SII;
 - (369.c) une description de la couche liaison de données du SII, y compris les protocoles et les paramètres d'encapsulation de la liaison de données.
- (370) L'entrepreneur doit s'assurer que les renseignements qu'il inscrit dans le DCI sont exacts et à jour.
- (371) L'entrepreneur doit apporter les modifications ou les mises à jour qui s'imposent dans le DCI dans les trois (3) JOGF.
- (372) L'entrepreneur doit émettre le DCI révisé et le présenter à SPC après révision.

8.9 Sécurité

- (373) L'entrepreneur doit, dans le JOGF suivant une demande présentée par SPC, fournir les registres de vérification en ligne relatifs au SII pour les emplacements que SPC précise ou qu'on lui demande, dans un format de fichier commercial déterminé par SPC.
- (374) L'entrepreneur doit, dans les cinq (5) JOGF suivant une demande présentée par SPC, fournir les registres de vérification archivés relatifs au SII pour les emplacements que SPC précise ou qu'on lui demande, dans un format de fichier commercial déterminé par SPC.
- (375) L'entrepreneur doit conserver les rapports sur les violations de la sécurité, les transactions et les journaux de vérification, les rapports d'incident d'alarme et les rapports connexes de l'année en cours et des deux années précédentes, et doit obtenir l'autorisation écrite de SPC avant de détruire tout rapport datant de plus de deux ans.
- (376) L'entrepreneur doit permettre à SPC, dans les dix (10) JOGF suivant une demande présentée par celui-ci, de se rendre dans ses locaux pour inspecter et vérifier sa conformité aux exigences prévues au contrat en matière de confidentialité, de sécurité et de gestion de l'information, et d'avoir pleinement accès à l'ensemble des dossiers et renseignements personnels pendant les JOGF, de 8 h à 17 h (HNE), et ce, sans frais pour SPC.
- (377) En cas d'incident lié à la sécurité, ou si SPC en fait la demande, l'entrepreneur doit prêter son concours à toute inspection ou vérification de la sécurité demandée par SPC, en fournissant l'information requise dans les dix (10) JOGF suivant la demande :
- (378) À la demande de SPC, l'entrepreneur doit lui donner accès à ses installations et à ses systèmes et lui fournir en temps opportun des preuves et une documentation suffisantes.
- (379) L'entrepreneur doit, à l'intérieur du délai précisé par SPC, se pencher sur les risques recensés dans l'application des processus de conformité de SPC en matière de sécurité et de confidentialité qui démontrent que les principes de sécurité et de confidentialité de SPC ont été compromis, ou qu'ils sont susceptibles d'être compromis.

8.10 Examen de la conformité

- (380) Chaque année, SPC peut procéder à un examen de la conformité qui comprend, entre autres, les éléments suivants :
- veiller à ce que le SII soit conforme aux exigences relatives à la sécurité;
 - s'assurer que tous les logiciels du SII possèdent une version à jour et actuelle des mises à jour et des correctifs de sécurité pour toutes les vulnérabilités connues;
 - vérifier que l'entrepreneur surveille de façon proactive les vulnérabilités des logiciels du SII et qu'il installe tout correctif de sécurité et toute nouvelle version des logiciels nécessaires à la correction de ces vulnérabilités;
 - s'assurer que l'entrepreneur examine quotidiennement les journaux de vérification de la sécurité.
- (381) L'entrepreneur doit fournir les pièces justificatives requises dans les dix (10) JOGF suivant une demande présentée par SPC dans le cadre de l'examen de la conformité.
- (382) Si SPC juge que les pièces justificatives ne démontrent pas le respect du contrat, il demandera à l'entrepreneur un plan dressant les mesures qu'il prendra pour régler les écarts relevés par rapport aux conditions générales du contrat.

9 GESTION DE LA QUALITÉ DU SERVICE

- (383) L'entrepreneur doit posséder un cadre de gestion de la qualité du service lui permettant de gérer le rendement de son service quant aux niveaux de service, aux plans de gestion des niveaux de service, aux rapports sur les niveaux de service, aux commandes de service, ainsi qu'aux opérations, à la surveillance, à la production de rapports, à la documentation connexe et à la facturation.
- (384) L'entrepreneur doit prendre les mesures requises en ce qui concerne son infrastructure ou son équipement de communication afin d'assurer le maintien de niveaux de service adéquats.
- (385) L'entrepreneur doit offrir un SII conformément aux niveaux de service définis au titre des exigences de rendement du service et spécifiés dans le tableau 7 de la section Gestion des niveaux de service.
- (386) L'entrepreneur doit surveiller et mesurer les niveaux de service, 24 heures sur 24, tous les jours de l'année.
- (387) L'entrepreneur doit fournir tout matériel et logiciel nécessaire à la surveillance et à la mesure des niveaux de service.
- (388) L'entrepreneur doit calculer et présenter les niveaux de service avec une précision de deux décimales, à moins d'indication contraire pour un niveau de service.
- (389) L'entrepreneur doit fournir à SPC l'accès aux renseignements de son service de gestion de l'information et à ses outils commerciaux de production de rapports pour surveiller les paramètres des niveaux de service qui sont essentiels afin d'assurer la qualité et la prestation du service.
- (390) L'entrepreneur doit fournir le SII et un service anti-déni de service distribué selon un niveau de disponibilité de 99,5 % mesuré sur une période d'un mois, 24 heures sur 24, tous les jours de l'année.
- (391) La « disponibilité » est un pourcentage basé sur le total du temps d'interruption du SII et le total du temps de service disponible, calculé comme suit :
- (Disponibilité du service attendue pour le mois - temps d'interruption durant le mois) × 100 % ÷ disponibilité du service attendue pour le mois*
- (392) L'entrepreneur doit présenter une justification ou une preuve écrite s'il ne parvient pas à respecter l'un des niveaux de service. SPC a l'autorisation d'accepter une justification écrite relative à une interruption attribuable à l'une des raisons suivantes :
- a) une défaillance des liaisons ou de l'équipement de télécommunication non fournis par l'entrepreneur;
 - b) des interruptions de maintenance prévues et approuvées par SPC;
 - c) une action posée par une ou plusieurs personnes qui ne relèvent pas de l'entrepreneur ou un accès retardé ou refusé de l'entrepreneur aux locaux du gouvernement du Canada lorsque l'entrepreneur doit se rendre sur place pour faire une réparation ou rétablir le service.

10 GESTION DES NIVEAUX DE SERVICE

10.1 Niveau de service – Accessibilité à Internet (NS-AI)

- (393) Le NS-AI du SII constitue le niveau de service de l'interconnexion Internet et de la disponibilité du service anti-déni de service distribué, selon lequel l'entrepreneur doit

s'assurer que le service est disponible et que les interruptions sont réduites au minimum, tel que défini au tableau 7 – Niveaux de service du SII.

10.1.1 Niveau de service – Temps d'interruption maximal du service (NS-TIMS)

- (394) Le NS-TIMS du SII et du service anti-déni de service distribué doit être équivalent ou inférieur à 216 minutes (soit 60 minutes × 24 heures × 30 jours × 0,005 ou environ l'équivalent d'une disponibilité de 99,5 %) de temps d'interruption cumulatif pour une période de 24 heures par jour pour chaque jour d'un mois donné (30 jours).
- (395) L'entrepreneur doit calculer le NS-TIMS du SII et le service anti-déni de service distribué en additionnant le temps d'interruption de tous les incidents survenus au cours du mois donné.
- (396) Le temps d'interruption du service attribuable à des problèmes de configuration découlant de travaux autorisés par SPC sera exclu du calcul du temps maximal d'interruption de service pour le SII.

10.1.2 Niveau de service – Délai maximal de rétablissement du service (NS-DMRS)

- (397) Le NS-DMRS du SII et le service anti-déni de service distribué est de quatre (4) heures.
- (398) Le calcul du NS-DMRS débute au moment où un incident causant une interruption du service en lien avec le SII et le service anti-déni de service distribué est relevé par SPC ou l'entrepreneur et se termine au moment de sa résolution.
- (399) Le calcul du NS-DMRS s'applique aux incidents lors desquels l'interruption survient indépendamment, que le délai maximal d'interruption de service ait été dépassé ou non pour un mois donné.

10.2 Niveau de service – Réponse aux commandes de service (NS-RCS)

- (400) Le NS-RCS du SII et le service anti-déni de service distribué est le niveau de service pour lequel on attend de l'entrepreneur qu'il exécute les commandes à l'intérieur d'une période déterminée dans la section de l'EDT sur les commandes de service. Si l'entrepreneur ne satisfait pas au NS-RCS en ne parvenant pas à fournir les éléments des DCS à l'intérieur d'un mois ou s'il les fournit en retard, il doit accorder le mois suivant un crédit pour les frais relatifs à chaque DCS qu'il n'a pu exécuter.

10.3 Niveau de service – Débit de données, délai de transit et perte de paquets

Les paramètres relatifs au débit de données (NS-DD), au délai de transit (NS-DT) et à la perte de paquets (NS-PP) sont définis dans le tableau 7 – Niveaux de services du SII.

10.4 Tableau des niveaux de service du SII

Paramètre du niveau de service	Descriptions	Exigence du niveau de service
Débit des données de paquets	<ul style="list-style-type: none"> ▪ L'entrepreneur doit mesurer le débit des données au PIS au moins toutes les 5 minutes, 24 heures par jour, tous les jours de l'année, et consigner les résultats sur son portail Web de sorte qu'ils soient accessibles au responsable technique. 	<p>En cas de panne chez un FAI, tout le trafic provenant d'Internet et allant vers celui-ci est automatiquement redirigé vers l'autre fournisseur et transmis par celui-ci. Puisque l'entrepreneur ne sera pas préalablement avisé d'une telle panne, son SII doit réagir à la situation automatiquement et sans heurts pour assurer l'accès à Internet. En tout temps, l'entrepreneur doit pouvoir prendre en charge du trafic IP supplémentaire selon le débit convenu.</p>
Délai de transit des paquets (NS – DT)	<ul style="list-style-type: none"> ▪ Délai de transit des paquets entre le SII et le point d'accès au réseau (voir la figure 2) – L'entrepreneur doit mesurer le délai de transit à sens unique en utilisant des paquets d'une taille maximale de 576 octets, à partir de son interface de SII respective vers chacune des interfaces du point d'accès au réseau pour lesquelles l'entrepreneur a des ententes d'homologage avec d'autres FAI. ▪ Délai de transit des paquets entre le SII et le PIS – L'entrepreneur doit mesurer le délai de transit à sens unique en utilisant des paquets d'une taille maximale de 576 octets, depuis son interface du SII vers le PIS. ▪ Des essais de mesure du délai de transit aller-retour sont acceptables si chaque résultat est divisé par deux pour obtenir le délai de transit à sens unique. ▪ L'entrepreneur doit mesurer le délai de transit des paquets dans les deux directions au moins toutes les 5 minutes, 24 heures par jour, tous les jours de l'année, et consigner les résultats sur son portail Web de sorte qu'ils soient accessibles au responsable technique. 	<p>Délai de transit entre le SII et le point d'accès au réseau – L'entrepreneur doit veiller à ce que le délai de transit des paquets à sens unique entre l'interface du SII et chaque interface du point d'accès au réseau (dans un rayon de 3000 km de l'interface du SII, au Canada et dans la zone continentale des États-Unis) ne dépasse pas 35 millisecondes pour au moins 95 % des paquets dans une heure donnée, y compris l'heure où le trafic est le plus important.</p> <p>Délai de transit entre le SII et le PIS – l'entrepreneur doit garantir que le délai de transit à sens unique entre le SII et le PIS ne dépasse pas 10 millisecondes pour au moins 95 % des paquets dans une heure donnée, y compris l'heure où le trafic est le plus important.</p>

Tableau 7 – Niveaux de service du SII

Paramètre du niveau de service	Descriptions	Exigence du niveau de service
<p>Perte de paquets de données (NS – PP)</p>	<ul style="list-style-type: none"> ▪ L'entrepreneur doit mesurer et consigner la perte de paquets de données depuis son interface du SII respective vers chaque interface du point d'accès au réseau, dans les deux directions et au moins toutes les 5 minutes, tous les jours, et consigner les résultats des mesures sur son portail Web de sorte qu'ils soient accessibles au responsable technique. 	<p>L'entrepreneur doit assurer la prestation du SII en offrant une perte de paquets de données ne dépassant pas 1 % entre l'interface du SII et chaque interface du point d'accès au réseau pendant une heure donnée.</p>
<p>Disponibilité</p>	<ul style="list-style-type: none"> ▪ Une interruption survient lorsque le réseau GC.Net ne peut pas communiquer avec Internet en raison d'une défaillance au sein du SII de l'entrepreneur respectif ou de l'infrastructure de ce dernier. ▪ Les mesures du délai de transit des paquets prises par l'entrepreneur seront également utilisées pour mesurer et surveiller la disponibilité du SII de l'entrepreneur respectif. Si deux essais relatifs au délai de transit consécutifs n'obtiennent pas de réponse d'une interface du point d'accès au réseau, l'entrepreneur doit consigner cet échec en tant qu'heure de début de l'interruption de service dans le dossier d'incident. La durée d'interruption du service commence à l'heure de début du problème et se termine lorsque l'interface du point d'accès au réseau correspondante répond au paquet de l'essai de délai de transit. Chaque période d'interruption de chaque mois est additionnée pour obtenir le temps d'interruption total du SII pour le mois. 	<ul style="list-style-type: none"> ▪ NS-DMRS : en cas d'interruption, l'entrepreneur doit remettre en marche le SII et le service anti-déni de service distribué dans les quatre heures à partir de l'heure d'interruption consignée dans le dossier d'incident. ▪ NS-TIMS : le SII de l'entrepreneur et le service anti-déni de service distribué doivent être offerts en tout temps, à l'exception d'un maximum de 40 minutes cumulatives d'interruption dans un mois civil donné.

Tableau 7 – Niveaux de service du SII (suite)

Service d'interconnexion Internet (SII) pour Services partagés Canada

Annexe A – Appendice A : Définitions et sigles

Date : Le 5 avril 2013

Version : D4

1 DÉFINITIONS

Terme	Définition
Adresse	Adresse municipale où se trouve un point de prestation de service (PPS).
Attaque par déni de service	Tentative de rendre une ressource informatique inaccessible à ses utilisateurs légitimes.
Authentification	Processus servant à vérifier qu'un utilisateur demeure propriétaire des justificatifs d'identité qui lui ont été remis, ou qu'il en garde le contrôle.
Gestion de la disponibilité	Processus visant à définir, à analyser, à planifier, à mesurer et à améliorer la disponibilité d'un service.
Secteur de la capitale nationale (SCN) du Canada	Installation dans un rayon de 100 km à partir du Parlement du Canada où le service est mis en œuvre.
Nord canadien	Installation située au 54 ^e parallèle, ou plus au nord, où le service est mis en œuvre.
Sud canadien	Installation située au sud du 54 ^e parallèle, excluant le SCN du Canada, où le service est mis en œuvre.
Certificat	Fichier électronique dont le format respecte la recommandation X.509 V3 de l'UIT-T, comme les jetons cryptographiques qu'EPF ou Entrust prend en charge, et qui comprend la clé publique d'un client (une personne ou un appareil), ainsi que de l'information connexe signée numériquement à l'aide de la clé privée de l'autorité de certification qui a émis le certificat.
Liste des certificats révoqués	Liste publiée et mise à jour par l'autorité de certification, qui présente les certificats qui ont été révoqués avant la fin de leur période de validité préétablie.
Certification	Évaluation des dispositifs de sécurité d'un système de TI et d'autres mesures de sauvegarde connexes, effectuée à l'appui de l'accréditation, afin de déterminer le degré selon lequel un modèle de conception et de mise en œuvre précis satisfait à un ensemble donné d'exigences relatives à la sécurité.
Autorité de certification (AC)	Entité sur qui la confiance d'au moins une autre entité repose afin de publier et de gérer les certificats de clés publiques X.509 et les listes de certificats révoqués. Selon le niveau d'assurance attribué à l'AC, celle-ci peut émettre, au sein de l'infrastructure à clés publiques (ICP) du gouvernement du Canada (GC), des certificats en fonction de politiques données.
Gestion des changements	Méthodes et procédures normalisées utilisées pour le traitement des changements apportés à une infrastructure ou à un service de

Terme	Définition
	TI en vue de minimiser le nombre d'incidents connexes lié au service et d'atténuer leur incidence.
Demande de changement	Demande visant à apporter des modifications au matériel, aux logiciels, aux applications ou aux processus que l'entrepreneur emploie en vue de fournir le service.
Dossier de changement	Moyen utilisé pour consigner une demande de changement.
Formation assistée par ordinateur (FAO)	Services de formation assistée par ordinateur fournis par l'entrepreneur, ce qui comprend la remise de documentation.
Élément de configuration (EC)	Tout composant d'une infrastructure de TI dont le contrôle est assuré au moyen de la gestion de la configuration. Les EC et leurs versions peuvent être gérés individuellement et sont habituellement traités comme des unités autonomes aux fins de désignation et de contrôle des changements.
Gestion de la configuration	Méthodes et procédures normalisées visant à contrôler les modifications apportées aux composants matériels et logiciels d'un système au cours de son cycle de vie.
Justificatif d'identité	Identificateur physique ou électronique exclusif associé à une personne.
Changement d'urgence	Demande de changement en vue d'effectuer le rétablissement opérationnel d'un service touché par une interruption ou une détérioration ayant une forte incidence sur la prestation de ce service, ou encore afin de corriger un incident de sécurité.
Mode FIPS	Un mode du module de chiffrement qui n'utilise que des fonctions de sécurité approuvées (à ne pas confondre avec un mode particulier d'une fonction de sécurité approuvée, p. ex., le mode de chiffrement par blocs chaîne de la norme Data Encryption Standard). En d'autres mots, lorsqu'un module est en mode FIPS, on ne peut pas utiliser une méthode qui n'est pas approuvée par la FIPS au lieu d'une qui l'est. Le certificat de validation FIPS 140-2 détermine le « mode d'opération FIPS » utilisé dans le module de chiffrement (source : FIPS 140-2).
Pare-feu	Barrière technologique conçue de façon à empêcher des communications non autorisées ou non désirées entre hôtes ou réseaux informatiques.
Hôte	Toute entité associée à une adresse IP et connectée à un réseau IP.
Incident	Tout événement qui ne s'inscrit pas dans le cadre de fonctionnement normal d'un service et qui cause ou peut causer une interruption de service ou une réduction de la qualité du service.

Terme	Définition
Gestion des incidents	Méthodes et procédures normalisées visant à rétablir le service normal le plus rapidement possible et à atténuer l'incidence opérationnelle.
Latence	Temps nécessaire à la transmission de paquets dans un réseau entre les points de départ et de destination. L'unité utilisée est le temps, mesuré en millisecondes (ms).
Service géré	Prestation d'un service à un client pour lequel le fournisseur est responsable d'assurer la prestation adéquate et qui doit respecter les niveaux de service prédéfinis du client.
Services de gestion	Services fournis par l'entrepreneur qui comprennent la gestion des changements, de la configuration, des incidents, des versions, de la capacité et de la disponibilité.
Temps d'interruption maximal du service	Temps maximal d'interruption cumulée attribuable à un incident ou plus au cours d'un mois civil.
Délai maximal de rétablissement du service	Délai maximum accordé pour rétablir un service dont l'interruption est causée par un incident.
Traduction d'adresses de réseau	Processus de modification de l'information d'une adresse IP en entêtes IP de paquets au cours de la transition de ces derniers dans un appareil d'acheminement du trafic.
Renseignements personnels	Tels que définis à l'article 3 de la <i>Loi sur la protection des renseignements personnels</i> .
Évaluation des facteurs relatifs à la vie privée (EFVP)	Outil d'évaluation décrivant le cheminement des renseignements personnels dans le cadre d'un projet et permettant d'analyser l'incidence que peut avoir ce cheminement sur le respect de la vie privée.
Gestion des versions	Méthodes et procédures normalisées visant l'intégration et le déroulement du développement, de la mise à l'essai, de la mise en œuvre et du soutien relatifs aux services fournis.
Atteinte à la sécurité	Accès physique ou logique non autorisé à un système d'information, qui a compromis la disponibilité, l'intégrité ou la confidentialité du système de TI.
Matrice de traçabilité des exigences relatives à la sécurité	Document employé afin de s'assurer qu'il est possible d'effectuer le suivi de toutes les exigences relatives à la sécurité comprises dans le système de TI au cours des étapes de conception, de mise en œuvre et de mise à l'essai dans le cadre du développement du système donné.
Essais des mécanismes de sécurité	Processus visant à confirmer que les mécanismes de sécurité techniques fonctionnent correctement.

Terme	Définition
Validation de la sécurité	Processus d'établissement de la correspondance, ou mappage, entre les exigences relatives à la sécurité et les procédures ou éléments de conception qui mettent en œuvre ou respectent ces exigences.
Vérification de la sécurité	Processus visant à confirmer la bonne mise en œuvre des mécanismes de sécurité proposés et des exigences en matière d'assurance.
Point de prestation de service	Un emplacement (c.-à-d. une adresse municipale) où on effectue la mise en œuvre d'une instance du service.
Conception du service	Conception du service préparée par l'entrepreneur pour chaque projet de service.
Délai de réponse du bureau de service	Délai nécessaire à l'agent du bureau de service de l'entrepreneur afin de répondre à un appel.
Niveau de service	Valeur employée afin d'évaluer le rendement, la disponibilité ou la qualité d'un service, d'un produit ou d'un système.
Niveau de service – Réponse à une demande de changement	Niveau de service relatif au délai de réponse dans le cas d'une demande de changement.
Niveau de service – Temps d'interruption maximal du service	Niveau de service relatif au temps d'interruption maximal d'un service.
Niveau de service – Temps d'interruption maximal du service (NS-TIMS)	Niveau de service relatif au temps d'interruption maximal du service offert.
Niveau de service – Délai maximal de présence sur place	Niveau de service quant au délai maximal alloué à un technicien afin qu'il arrive sur place, à partir du moment où un problème est signalé.
Niveau de service – Délai maximal de rétablissement du service (NS-DMRS)	Niveau de service relatif au délai maximal accordé afin de rétablir le service, une fois qu'un problème a été signalé.
Niveau de service – Disponibilité du centre des opérations	Niveau de service relatif à la disponibilité du centre des opérations.
Niveau de service – Rendement	Niveau de service relatif au débit de traitement des données, au délai de livraison des paquets et à la perte de paquets.
Niveau de service – Délai de réponse à une commande de service	Niveau de service relatif au délai de réponse dans le cas d'une demande de commande de service.

Terme	Définition
Niveau de service – Disponibilité du portail de service	Niveau de service quant à la disponibilité du portail du service.
Plan de gestion du service	Plan indiquant quels services de gestion l'entrepreneur doit fournir.
Délai de réponse à une commande de service	Le nombre de jours ouvrables du gouvernement fédéral compris entre la date de remise de la commande de service à l'entrepreneur et le moment où le responsable technique donne son acceptation des travaux pour ce service.
Portail de service	Portail de service fourni et géré par l'entrepreneur, ce qui comprend la documentation connexe.
Disponibilité du portail de service	Le pourcentage de temps pendant lequel le portail de service est entièrement opérationnel.
Plan de projet de service	Plan du projet de service préparé par l'entrepreneur pour chaque projet de service.
Version de service	Version du logiciel qui est conçue pour fonctionner sur des combinaisons données de matériel informatique et de systèmes d'exploitation. En général, on indique une nouvelle version de système en ajoutant le chiffre « 1 » au premier chiffre du numéro de version (p. ex., v.2.X.X serait la version de système suivante après la version v.1.X.X).
Évaluation de la menace et des risques (EMR)	Processus structuré conçu dans le but de déterminer les risques et de fournir des recommandations afin d'atténuer les risques au moyen de l'analyse des aspects essentiels des systèmes et des services, des événements ou scénarios de menace potentiels et des vulnérabilités inhérentes.
Capacité de gestion des risques	Appareils physiques, virtuels ou combinaison des deux, capables de fournir tous les services de gestion des risques à une vitesse de câble déterminée.
Service de gestion des risques	<p>Un service de sécurité, parmi la liste ci-dessous, qu'il est possible d'activer dans le cadre de la capacité de gestion des risques :</p> <ul style="list-style-type: none"> • pare-feu; • détection et prévention des intrusions; • filtrage du contenu; • antivirus; • antipourriel; • protection contre la perte de données.
Mode tunnel	Configuration qui empêche un appareil utilisateur d'accéder à un réseau public (p. ex., Internet) pendant l'utilisation d'un tunnel de RPV (réseau local à distance).
Mise à niveau	Mise à jour du logiciel sous licence pour étoffer, étendre, rehausser ou améliorer les caractéristiques, la fonctionnalité ou le rendement

Terme	Définition
	du code du programme du logiciel. Les mises à niveau sont documentées par une modification du numéro de version ou du numéro d'identification à la droite de la première décimale (p. ex., le produit X, version 1.0, devient le produit X, version 1.1, ou encore le produit X, version 1.0.0, devient le produit X, version 1.0.1), peu importe si l'entrepreneur mentionne ou non qu'il s'agit d'une mise à niveau « mineure » ou « majeure ».
Utilisateur	Personne qui utilise le service.
Appareil utilisateur	Appareil électronique d'un utilisateur qui lui permet de se connecter au service.
Réseau local virtuel (RLV)	Partition réseau logique pour un RL.
Réseau virtuel (RV)	Partition réseau logique.
Routage et acheminement virtuel	Technologie qui permet la coexistence de multiples instances de tables de routage au sein du même routeur, en même temps.
Débit du trafic virtuel	Trafic contractuel attribué à un réseau virtuel.
Tunnel RPV	Connexion servant à transmettre des données de façon sécurisée au sein d'un réseau non sécurisé, comme Internet. Un tunnel RPV est dit « virtuel », car il ne nécessite pas de lignes dédiées. Il est « privé », car on le chiffre afin de le sécuriser.
Évaluation des vulnérabilités	Processus visant à déterminer l'existence de vulnérabilités dans le système.
Point d'accès sans fil	Appareil qui permet aux hôtes autorisés de se connecter à un réseau à l'aide des normes de réseau sans fil.
Vitesse du câble	Lorsque les données sont transmises à la vitesse du câble, ou au débit du câble, cela signifie qu'il n'y pas ou peu de temps système de logiciel associé à la transmission et que les données se déplacent à la vitesse maximale permise par le matériel employé.
Incident lié à la sécurité	<p>Type d'incident. Plus précisément, il s'agit d'une violation ou d'un risque imminent de violation des politiques de sécurité informatique, des politiques relatives à l'utilisation acceptable ou des pratiques normalisées en matière de sécurité, qui peut avoir une incidence négative, comme des pannes du système, une saturation des paquets sur le réseau, l'utilisation non autorisée de privilèges réseau, l'accès non autorisé à des données de nature délicate ou l'exécution de codes malveillants entraînant la destruction de données.</p> <p>ou</p> <p>Comportement non autorisé (selon la politique de sécurité du système de TI) quant à l'exploitation et à l'administration du système pouvant compromettre la confidentialité, l'intégrité ou la disponibilité de celui-ci.</p>

2 SIGLES

Acronyme	Terme
ADSL ou LNPA	Ligne numérique à paire asymétrique
AES	Algorithme Advanced Encryption Standard (norme sur le chiffrement perfectionné)
AM	<i>ante meridiem</i> (utilisé en anglais seulement). Origine latine, signifie l'intervalle de temps entre minuit et midi.
LAR	Liste d'autorités révoquées
AS	Système autonome (utilisé en anglais seulement)
BGP	Protocole BGP (Border Gateway Protocol)
AC	Autorité de certification
CIR	Débit minimal garanti (utilisé en anglais seulement)
COTS	Commercial (utilisé en anglais seulement)
LCR	Liste des certificats révoqués
DFPS	Date ferme de prestation du service
CSTC	Centre de la sécurité des télécommunications Canada
CSV	Format Comma-separated values
DOS	Déni de service
DDOS	Déni de service distribué
DES	Data Encryption Standard (norme de chiffrement des données, États-Unis)
DHCP	Protocole DHCP (Dynamic Host Configuration Protocol)
DiffServ	Services différenciés
DNS	Système de noms de domaine
DOS	Déni de service
EAL	Norme Evaluated Assurance Level (niveau d'assurance de l'évaluation)
EIA	Electronic Industries Alliance
VAF	Vérification approfondie de la fiabilité
ESP	Protocole ESP (Encapsulating Security Payload)
HNE	Heure normale de l'Est (Canada)
FAX	Télécopieur
JOGF	Jours ouvrables du gouvernement fédéral

Acronyme	Terme
FIPS	Federal Information Processing Standard (normes fédérales de traitement de l'information)
FTP	Protocole de transfert de fichiers
FOCIS	Fiber Optic Connector Intermateability Standard (norme d'interopérabilité des connecteurs à fibre optique)
Gbit/s	Gigabit par seconde
GC	Gouvernement du Canada
GCNet	Réseau du gouvernement du Canada
HTML	Langage de balisage hypertexte
HTTP et HTTPS	Protocole de transfert hypertexte et protocole de transfert hypertexte sécurisé
DCI	Document de contrôle d'interface
ICMP	Protocole de message de contrôle Internet
IEEE	Institute of Electrical and Electronic Engineers
CEI	Commission électrotechnique internationale
IETF	Internet Engineering Task Force
IKE	Protocole IKE (Internet Key Exchange)
SII	Service d'interconnexion Internet
IP	Protocole Internet
IPSec	Protocole IPSec (Internet Protocol Security)
ISO	Organisation internationale de normalisation
FAI	Fournisseur d'accès Internet
DGSIT	Direction générale des services d'infotechnologie
ITSG	Conseils en matière de sécurité de TI
RL	Réseau local
LDAP	Protocole LDAP (Lightweight Directory Access Protocol)
LIAS	Service d'accès internet local (utilisé en anglais seulement)
MAT	Débit mensuel moyen (utilisé en anglais seulement)
MD	Condensé de message (utilisé en anglais seulement)
PMR	Prix mensuel récurrent
DMR	Durée moyenne des réparations
CAR	Contrôle d'accès au réseau

Acronyme	Terme
NACR	Demandes de changement d'annonce de réseau (utilisé en anglais seulement)
NAP	Point d'accès au réseau (utilisé en anglais seulement)
NAT	Traduction d'adresses de réseau
NetBIOS	Système de base d'entrée-sortie de réseau
COR	Centre des opérations de réseau
FINR	Frais d'installation non récurrents
OGD	Autre ministère (utilisé en anglais seulement)
PPO	Plan de préparation opérationnelle
ZAP	Zone d'accès public
PDP	Perte des données de paquet
DLP	Délai de livraison des paquets
EFVP	Évaluation des facteurs relatifs à la vie privée
ICP	Infrastructure à clés publiques
PDS	Point de service
RTCP	Réseau téléphonique commuté public
QOS	Qualité de service
RADB	Base de données Random Arbiter Data Base
ACF	Analyse des causes fondamentales
RFC	Demande de commentaires
RPC	Protocole d'appel de procédures à distance
RPSL	Langage RPSL (Routing Policy Specification Language)
SAN	Numéro de l'autorité de Services partagés Canada (utilisé en anglais seulement)
SPC	Services partagés Canada
DPS	Délai de prestation du service
PPS	Point de prestation de service
PIS	Point d'interface des services
SLMP	Plan de gestion des niveaux de service
SMTP	Protocole SMTP (Simple Mail Transfer Protocol)
SNMP	Protocole SNMP (Simple Network Management Protocol)
AECS	Avis d'exécution de la commande de service

Acronyme	Terme
SOA	Acceptation de la commande service (utilisé uniquement en anglais)
DCS	Demande de commande de service
EDT	Énoncé des travaux
ADP	Accès à distance protégé
MTERS	Matrice de traçabilité des exigences relatives à la sécurité
SSD	Bureau de service de SPC (utilisé en anglais seulement)
SSL	Protocole SSL (Secure Sockets Layer)
RT	Responsable technique
SCT	Secrétariat du Conseil du Trésor du Canada
TCP	Protocole de contrôle de transmission
Telnet	Protocole qui permet à des terminaux d'ordinateurs éloignés de se connecter à un serveur à l'aide d'un réseau TCP/IP, comme Internet
TIA	Telecommunications Industry Association
TLS	Protocole TLS (Transport Layer Security)
EMR	Évaluation de la menace et des risques
ATS	Appareil de télécommunication pour sourds
TTY	Téléimprimeur
UBR	Débit binaire non spécifié
UDP	Protocole UDP (User datagram protocol)
URL	Localisateur de ressources uniformes
RLV	Réseau local virtuel
RPV	Réseau privé virtuel
XML	Langage de balisage extensible



Government of Canada
Gouvernement du Canada

Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

**SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)**

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE			
1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine Shared Services Canada		2. Branch or Directorate / Direction générale ou Direction Transformation and Services Strategy Design	
3. a) Subcontract Number / Numéro du contrat de sous-traitance		3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant	
4. Brief Description of Work / Brève description du travail Internet Interconnect Services (IIS), to replace diverse and redundant Internet services under the expiring SCNet contracts.			
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?		<input checked="" type="checkbox"/> No Non	<input type="checkbox"/> Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?		<input checked="" type="checkbox"/> No Non	<input type="checkbox"/> Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis			
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)		<input type="checkbox"/> No Non	<input checked="" type="checkbox"/> Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.		<input checked="" type="checkbox"/> No Non	<input type="checkbox"/> Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?		<input checked="" type="checkbox"/> No Non	<input type="checkbox"/> Yes Oui
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès			
Canada	<input checked="" type="checkbox"/>	NATO / OTAN	<input type="checkbox"/>
		Foreign / Étranger	<input type="checkbox"/>
7. b) Release restrictions / Restrictions relatives à la diffusion			
No release restrictions Aucune restriction relative à la diffusion	<input checked="" type="checkbox"/>	All NATO countries Tous les pays de l'OTAN	<input type="checkbox"/>
Not releasable À ne pas diffuser	<input type="checkbox"/>		
Restricted to: / Limité à:	<input type="checkbox"/>	Restricted to: / Limité à:	<input type="checkbox"/>
Specify country(ies): / Préciser le(s) pays:		Specify country(ies): / Préciser le(s) pays:	
7. c) Level of information / Niveau d'information			
PROTECTED A PROTÉGÉ A	<input checked="" type="checkbox"/>	NATO UNCLASSIFIED NATO NON CLASSIFIÉ	<input type="checkbox"/>
PROTECTED B PROTÉGÉ B	<input type="checkbox"/>	NATO RESTRICTED NATO DIFFUSION RESTREINTE	<input type="checkbox"/>
PROTECTED C PROTÉGÉ C	<input type="checkbox"/>	NATO CONFIDENTIAL NATO CONFIDENTIEL	<input type="checkbox"/>
CONFIDENTIAL CONFIDENTIEL	<input type="checkbox"/>	NATO SECRET NATO SECRET	<input type="checkbox"/>
SECRET SECRET	<input type="checkbox"/>	COSMIC TOP SECRET COSMIC TRÈS SECRET	<input type="checkbox"/>
TOP SECRET TRÈS SECRET	<input type="checkbox"/>		
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT)	<input type="checkbox"/>		
		PROTECTED A PROTÉGÉ A	<input type="checkbox"/>
		PROTECTED B PROTÉGÉ B	<input type="checkbox"/>
		PROTECTED C PROTÉGÉ C	<input type="checkbox"/>
		CONFIDENTIAL CONFIDENTIEL	<input type="checkbox"/>
		SECRET SECRET	<input type="checkbox"/>
		TOP SECRET TRÈS SECRET	<input type="checkbox"/>
		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT)	<input type="checkbox"/>



Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? No / Non Yes / Oui
Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

- | | | | |
|---|---|---|--|
| <input checked="" type="checkbox"/> RELIABILITY STATUS
COTE DE FIABILITÉ | <input type="checkbox"/> CONFIDENTIAL
CONFIDENTIEL | <input type="checkbox"/> SECRET
SECRET | <input type="checkbox"/> TOP SECRET
TRÈS SECRET |
| <input type="checkbox"/> TOP SECRET - SIGINT
TRÈS SECRET - SIGINT | <input type="checkbox"/> NATO CONFIDENTIAL
NATO CONFIDENTIEL | <input type="checkbox"/> NATO SECRET
NATO SECRET | <input type="checkbox"/> COSMIC TOP SECRET
COSMIC TRÈS SECRET |
| <input type="checkbox"/> SITE ACCESS
ACCÈS AUX EMPLACEMENTS | | | |

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No / Non Yes / Oui
If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté? No / Non Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? No / Non Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? No / Non Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? No / Non Yes / Oui



Contract Number / Numéro du contrat 10026415
Security Classification / Classification de sécurité Unclassified

PART C - (continued) / PARTIE C - (suite)

For users completing the form manually use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire manuellement doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC						
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ			CONFIDENTIAL	SECRET	TOP SECRET	
				CONFIDENTIEL	TRÈS SECRET	NATO DIFFUSION RESTREINTE	NATO CONFIDENTIEL		A		B	C	CONFIDENTIEL		TRÈS SECRET		
Information / Assets Renseignements / Biens Production	✓																
IT Media / Support TI	✓																
IT Link / Lien électronique	✓																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED? No / Yes
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? Non / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED? No / Yes
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? Non / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).