Annexe A : Énoncé des travaux

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

Date : Le 6 mai 2013

TABLE DES MATIÈRES

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.

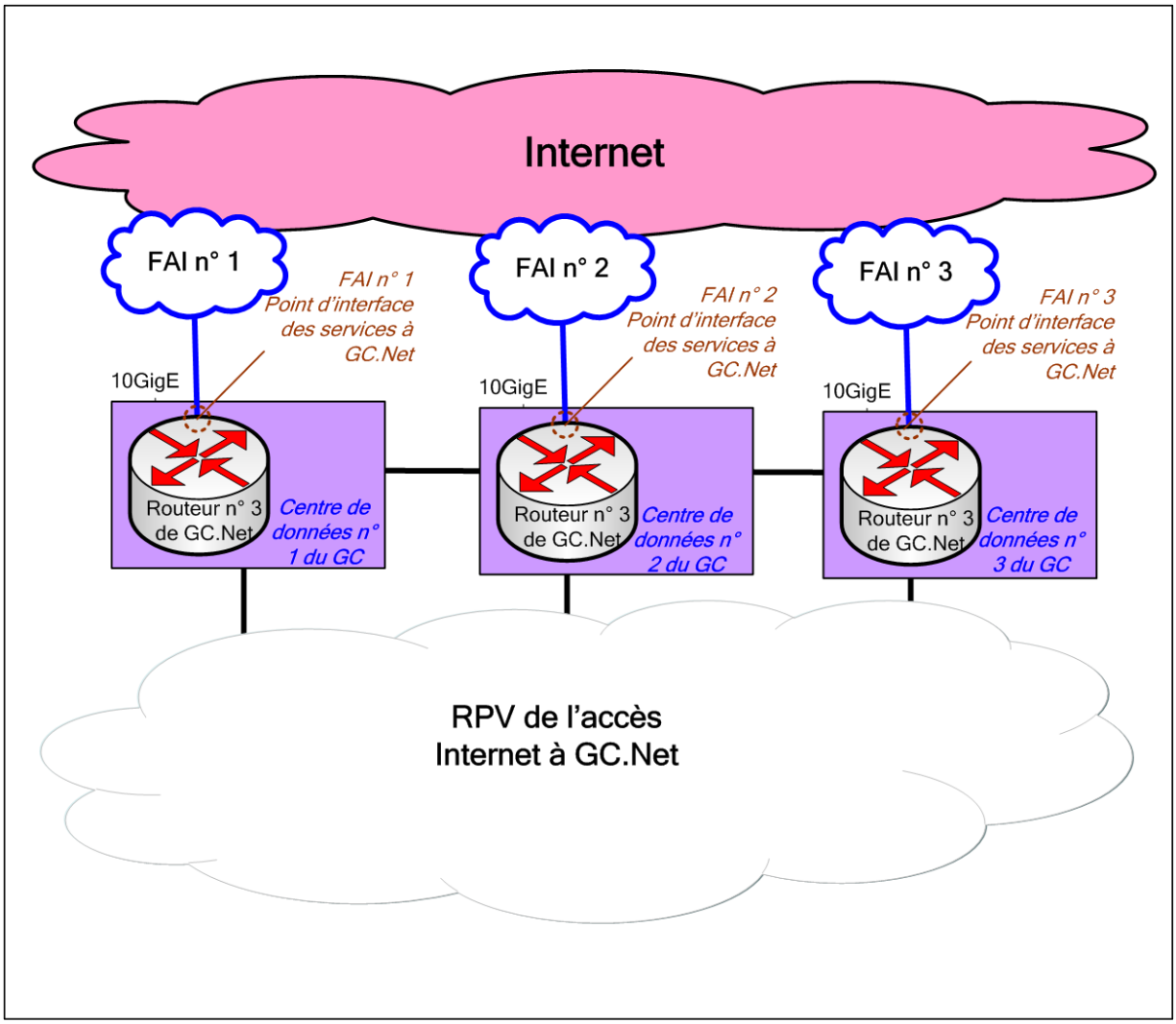

Figure 1: Infrastructure Internet du réseau du Canada

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.

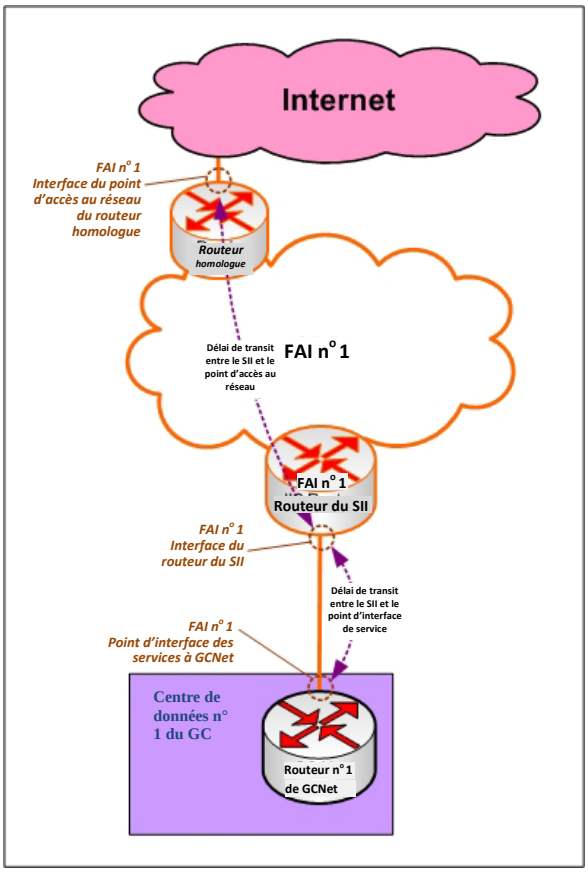

Figure 2 : Délai de transit entre le SII et le point d'accès au réseau et entre le SII et le PIS

(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 échelonnable, 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.

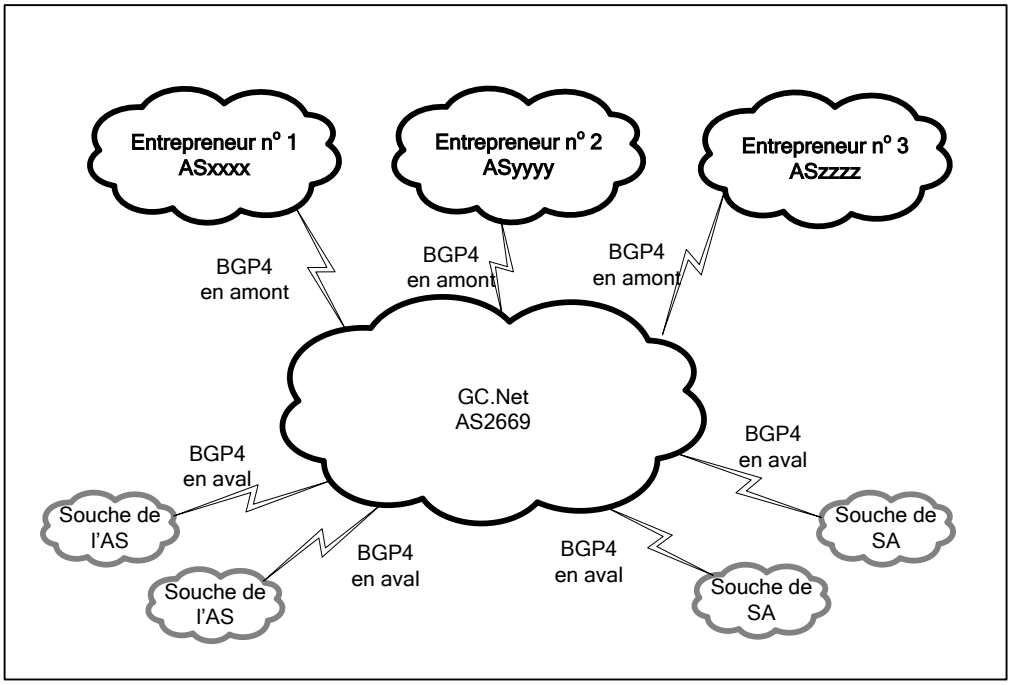

Figure 3 : Systèmes autonomes du réseau du Canada

(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 cyber-menace imminente. Une fois la menace ciblée, l'entrepreneur doit prendre des mesures immédiates, conformément à la section 5.3, Gestion des incidents, afin de mettre en application les recommandations visant à offrir une protection contre les cyber-menaces en modifiant la configuration et les seuils du système et en consignant le tout dans les rapports après incident aux fins de protection et de diligence raisonnable contre de futurs scénarios de cyber-menaces potentiels.

(92) L'entrepreneur doit fournir à SPC les coordonnées d'une personne-ressource qui répondra aux questions, discutera des cyber-menaces 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 sur la sécurité de l'intégration;
   ii) Plan d'évaluation des vulnérabilités;
   iii) Plan de vérification de l'installation des composants de sécurité;
   iv) Rapport d'essai sur la sécurité de l'intégration;
   v) Rapport d'évaluation des vulnérabilités;
   vi) 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 :

a) un diagramme détaillé des composants (c'est-à-dire une version approfondie du diagramme de haut niveau);

b) la description de la répartition des mécanismes de sécurité techniques entre les éléments de conception détaillée du service;

c) la description de la répartition de tous les mécanismes de sécurité non techniques parmi les éléments organisationnels ou opérationnels de haut niveau;

d) 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 Évaluation de la sécurité et autorisation de l'installation

(134) Dans les trente (65) JOGF suivant l'adjudication du contrat, l'entrepreneur doit soumettre à l'approbation de SPC une version provisoire des livrables suivants :

a) plan d'essai de la sécurité de l'intégration (voir la sous-section Plan d'essai de la sécurité de l'intégration);
b) plan d'évaluation des vulnérabilités (voir la sous-section Plan d'évaluation des vulnérabilités);
c) plan de vérification de l'installation des composants de sécurité (voir la sous-section Plan de vérification de l'installation des composants de sécurité);
d) rapport d'essai sur la sécurité de l'intégration (voir la sous-section Rapport d'essai sur la sécurité de l'intégration);
e) rapport d'évaluation des vulnérabilités (voir la sous-section Rapport d'évaluation des vulnérabilités);
f) rapport de vérification de l'installation des composants de sécurité (voir la sous-section Rapport de vérification de l'installation des composants de sécurité).

(135) L'entrepreneur doit attendre l'approbation de l'étape 3 par SPC avant de déclarer le SII prêt à l'emploi.

3.6.3.2 Plan d'essai de la sécurité de l'intégration

(136) L'entrepreneur doit élaborer un plan d'essai de la sécurité de l'intégration qui porte sur les fonctions de sécurité intégrées.

(137) Le plan d'essai de la sécurité de l'intégration doit dresser la liste des essais à effectuer et décrire le déroulement de chacun d'eux. La portée du scénario d'essai doit s'étendre aux liens de dépendance envers les résultats d'autres essais.

(138) L'entrepreneur doit prendre les dispositions nécessaires pour permettre aux représentants du Canada d'assister aux essais de la sécurité de l'intégration.

(139) L'entrepreneur doit fournir à SPC un plan d'essai de la sécurité de l'intégration qui contient au moins les renseignements suivants :

a) les fonctions de sécurité faisant l'objet d'essais;
b) les dispositions nécessaires pour permettre aux représentants du Canada d'assister aux essais de la sécurité de l'intégration;
c) les éléments pour chaque fonction de sécurité ou ensemble de fonctions de sécurité faisant l'objet d'essais, y compris :
    i) la description de chaque scénario et procédure d'essai;

ii) les exigences en matière d'environnement;
iii) les liens de dépendance;
iv) les résultats attendus (c.-à-d. des critères de type réussite/échec).

(140) L'entrepreneur doit fournir à SPC une matrice de traçabilité à jour des exigences en matière de sécurité, qui contient les renseignements suivants sur chacune des exigences faisant l'objet d'essais dans le cadre du plan d'essai de la sécurité de l'intégration :

a) une référence à chaque élément identifiable dans les scénarios d'essai de l'intégration.

3.6.3.3 Plan d'évaluation des vulnérabilités

(141) L'entrepreneur doit fournir à SPC un plan d'évaluation des vulnérabilités qui contient au moins les renseignements suivants :

a) une description de la portée de l'évaluation des vulnérabilités;
b) les dispositions nécessaires pour permettre aux représentants du Canada d'assister à l'évaluation des vulnérabilités;
c) une description du processus d'évaluation des vulnérabilités;
d) une description des outils qui serviront à évaluer les vulnérabilités, y compris le numéro de version des divers logiciels employés.

3.6.3.4 Plan de vérification de l'installation des composants de sécurité

(142) L'entrepreneur doit élaborer un plan de vérification de l'installation des composants de sécurité en vue de procéder à une évaluation exhaustive de l'installation et de la configuration des composants de sécurité de l'environnement de production du SII.

(143) Le plan de vérification de l'installation des composants de sécurité doit dresser la liste des vérifications à effectuer et décrire le déroulement de chacune d'elles.

(144) L'entrepreneur doit prendre les dispositions nécessaires pour permettre aux représentants du Canada d'assister à la vérification de l'installation des composants de sécurité.

(145) L'entrepreneur doit fournir à SPC un plan de vérification de l'installation des composants de sécurité qui contient au moins les renseignements suivants :

a) l'approche adoptée pour vérifier la sécurité;
b) les dispositions nécessaires pour permettre aux représentants du Canada d'assister à la vérification de l'installation des composants de sécurité;
c) une description des composants de sécurité vérifiés;
d) pour chacun des composants de sécurité vérifiés :
    i) une description du scénario de vérification;
    ii) les liens de dépendance;
    iii) les résultats attendus (c.-à-d. des critères de type réussite/échec).

(146) L'entrepreneur doit fournir à SPC une matrice de traçabilité à jour des exigences en matière de sécurité, qui contient les renseignements suivants sur chacune des exigences faisant l'objet d'essais dans le cadre du plan de vérification de la sécurité des composants de sécurité:

a) une référence à chaque élément identifiable dans les scénarios de vérification de l'installation des composants de sécurité.

3.6.3.5 Rapport d'essai sur la sécurité de l'intégration

(147) L'entrepreneur doit faire l'essai de la sécurité de l'intégration, conformément au plan d'essai de la sécurité de l'intégration.

(148) L'entrepreneur doit fournir à SPC un rapport d'essai sur la sécurité de l'intégration, qui contient au moins les renseignements suivants sur chacun des éléments du plan d'essai de la sécurité de l'intégration :

a) les résultats attendus (c.-à-d. des critères de type réussite/échec);
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

3.6.3.6 Rapport d'évaluation des vulnérabilités

(149) L'entrepreneur doit évaluer les vulnérabilités, conformément au plan d'évaluation des vulnérabilités.

(150) L'entrepreneur doit installer des correctifs ou mettre en œuvre des mesures correctives dans le cadre de cette évaluation des vulnérabilités. S'il n'est pas en mesure de réaliser cette évaluation (p. ex., le temps requis pour faire l'essai du correctif ou pour déterminer les mesures correctives nécessaires et en faire l'essai entraînerait un retard important dans l'échéancier du projet), l'entrepreneur doit créer un ticket de gestion des changements lorsque l'installation d'un correctif ou la mise en place d'une mesure corrective est impossible à réaliser dans le cadre de l'évaluation des vulnérabilités. De tels tickets doivent être créés dans le système de gestion des changements de l'environnement de production en vue de les mettre en œuvre au cour de la phase en service du contrat.

(151) L'entrepreneur doit fournir à SPC un rapport d'évaluation des vulnérabilités, qui contient au moins les renseignements suivants :

a) une liste des essais d'évaluation des vulnérabilités réalisés;
b) pour chacun des essais d'évaluation des vulnérabilités :
   i) l'indication qu'une vulnérabilité connue a été relevée;
   ii) une description de la vulnérabilité;
   iii) une description du correctif installé ou de la mesure corrective mise en place pour éliminer la vulnérabilité;
c) pour chacune des vulnérabilités qui n'ont pas été éliminées :
   i) une évaluation des conséquences de la vulnérabilité dans le contexte des services SII de SPC;
   ii) le numéro de dossier d'incident associé au correctif ou à la mesure corrective en suspens, ou
   iii) la raison pour laquelle le correctif n'a pas été installé ou la mesure corrective n'a pas été mise en place.

3.6.3.7 Rapport de vérification de l'installation des composants de sécurité

(152) L'entrepreneur doit vérifier l'installation des composants de sécurité, conformément au plan de vérification de l'installation des composants de sécurité.

(153) L'entrepreneur doit corriger les erreurs et omissions ayant trait à l'installation ou à la configuration relevées dans le cadre de la vérification de l'installation des composants de sécurité.

(154) L'entrepreneur doit fournir à SPC un rapport de vérification de l'installation des composants de sécurité, qui contient au moins les renseignements suivants sur chacun des éléments du plan de vérification de l'installation des composants de sécurité :

a) les résultats attendus (c.-à-d. des critères de type réussite/échec);
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

3.6.4 Concept des opérations de sécurité

(155) 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

(156) 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

(157) 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/itsg 22-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 a voir 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

(158) 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

(159) 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

(160) 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.

(161) 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

(162) L'entrepreneur doit fournir les composants du SII et en assurer l'entretien.

(163) L'entrepreneur doit mettre en œuvre le SII aux emplacements indiqués par SPC.

(164) 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/);

(165) 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.

(166) 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

(167) L'entrepreneur doit présenter à SPC des rapports hebdomadaires sur l'état d'avancement de la mise en œuvre du SII.

(168) 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

(169) Le plan de mise en œuvre doit comprendre les trois (3) jalons suivants :

(169.a) conception préliminaire;

(169.b) conception critique;

(169.c) examen de la préparation opérationnelle.

3.7.2.1 Conception préliminaire

(170) 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.

(171) 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.

(172) L'entrepreneur doit documenter la visite du site et transmettre son rapport au Canada dans les deux (2) JOGF suivant la visite.

(173) La conception préliminaire est terminée lorsque SPC approuve la visite du site.

3.7.2.2 Conception critique

(174) 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).

(175) 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.

(176) 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.

(177) L'entrepreneur doit indiquer si les renseignements fournis sont considérés comme exclusifs.

(178) Après la réception du document de configuration du SII, l'entrepreneur doit rencontrer SPC pour discuter de tout problème décelé dans le document.

(179) En fonction des commentaires formulés par SPC, l'entrepreneur doit soumettre à son approbation une version finale du document de configuration du SII.

(180) 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.

(181) L'entrepreneur doit présenter toute modification du document et obtenir l'approbation de SPC pour ces modifications dans les cinq (5) JOGF.

(182) 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.

(183) L'entrepreneur doit présenter à SPC ses procédures relatives aux opérations et à la gestion du service à cette étape.

(184) 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

(185) 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.

(186) L'entrepreneur doit soumettre à l'approbation de SPC les versions finales des procédures de gestion des opérations et du service.

(187) 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.

(188) 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 :

(188.a) utiliser les commandes « ping » et « traceroute » ou toute autre procédure nécessaire pour tester la connectivité du réseau;

(188.b) vérifier que les numéros de réseau à transmettre à l'ensemble du réseau Internet sont transmis correctement;

(188.c) vérifier que les numéros de réseau qui ne doivent pas être transmis à l'ensemble du réseau Internet ne sont pas transmis;

(188.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;

(188.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.

(189) 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.

(190) 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

(191) 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

(192) Le SII doit prendre en charge les certificats fournis par SPC.

3.7.4 Connectivité de réseau

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

4 GESTION DU SERVICE

(194) 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.

(195) 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.

(196) 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.

(197) 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

(198) 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.

(199) 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.

(200) 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.

(201) 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.

(202) L'entrepreneur doit assurer la transition entre le centre principal et le centre de relève selon le plan de continuité du service.

(203) 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

(204) 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.

(205) 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.

(206) 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

(207) 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).

(208) 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.

(209) 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).

(210) 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.

(211) 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.

(212) 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.

(213) 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.

(214) 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.

(215) 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.

(216) L'entrepreneur doit être en mesure de suivre, de surveiller et de signaler tout problème ayant une incidence sur le service.

(217) 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.

(218) 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.

(219) L'entrepreneur doit assister à des réunions pour discuter des problèmes ayant une incidence sur la prestation des services et pour les résoudre.

(220) Les experts techniques de l'entrepreneur doivent assister aux réunions au besoin.

(221) 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

(222) 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.

(223) 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.

(224) 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.

(225) 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.

(225.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;

(225.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;

(225.c) afin de confirmer la réalisation des travaux et le rétablissement du service;

(225.d) afin de transmettre par courriel un avis au responsable technique décrivant les travaux et confirmant leur réalisation.

(226) 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.

(227) 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.

(228) L'entrepreneur doit travailler en collaboration avec SPC et d'autres entrepreneurs du SII afin de résoudre les incidents et les problèmes.

(229) 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.

(230) 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.

(231) 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.

(232) 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.

(233) 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.

(234) 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

(235) 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.

(236) 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.

(237) 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.

(238) L'entrepreneur doit fournir le personnel nécessaire à la réalisation d'entrevues, de même que tous les renseignements requis pendant la vérification.

(239) 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.

(240) Tout au long du cycle de vie du SII, l'entrepreneur doit :

a) atténuer les risques de façon à les maintenir à niveau acceptable selon SPC;

b) 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;

c) procéder à une évaluation et à une autorisation de sécurité conformément au contrat;

d) 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.

(241) Le programme d'inspection doit comprendre, entre autres, les éléments suivants :

a) des analyses visant à repérer les vulnérabilités des systèmes d'exploitation et des réseaux, authentifiés ou non;

b) des analyses visant à repérer les vulnérabilités des applications Web, authentifiées ou non;

c) des analyses visant à repérer les vulnérabilités des applications de base de données, authentifiées ou non.

(242) 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

(243) L'entrepreneur doit fournir tous les composants nécessaires à la prestation des services de gestion associés au SII, sans frais supplémentaires pour SPC.

(244) L'entrepreneur doit fournir des services de gestion associés au SII sans frais supplémentaires pour SPC.

(245) 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.

(246) 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.

(247) L'entrepreneur doit soumettre un avis à SPC et obtenir son approbation dix (10) JOGF avant l'exécution des travaux.

(248) 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

(249) 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.

(250) Toutes les demandes de changement doivent être approuvées par SPC.

(251) 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.

(252) 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.

(253) 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.

(254) L'entrepreneur doit exécuter les demandes de changement non urgentes durant les périodes de maintenance approuvées par SPC.

(255) L'entrepreneur doit transmettre les demandes de changement aux échelons supérieurs lorsque SPC l'exige.

(256) 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.

(257) 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.

(258) 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).

(259) 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.

(260) 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.

(261) 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.

(262) 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.

(263) L'entrepreneur doit envoyer à SPC un avis d'annulation de demande de changement, au plus tard 24 heures après avoir annulé la demande.

(264) 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.

(265) 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.

(266) 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.

(267) L'entrepreneur doit fermer le dossier de changement lié à une demande de changement une fois que celle-ci a été acceptée par SPC.

(268) 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.

(269) 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

(270) 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

(271) 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.

(272) 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.

(273) 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.

(274) 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.

(275) L'entrepreneur doit fournir à SPC les notifications d'incident selon les matrices de gestion et d'opération relatives à l'acheminement.

(276) L'entrepreneur doit changer l'échelon de transmission propre à un incident dans les 15 minutes suivant une demande de SPC.

(277) L'entrepreneur doit créer un dossier d'incident pour chaque incident.

(278) 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.

(279) 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.

(280) 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).

(281) 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.

(282) L'entrepreneur doit mettre à jour le journal d'information sur les dossiers d'incident à la suite d'un changement d'état.

(283) 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.

(284) 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.

(285) L'entrepreneur doit faire le suivi de la durée d'interruption liée à chaque incident et l'inscrire dans les dossiers d'incident correspondants.

(286) 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.

(287) 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.

(288) L'entrepreneur doit suspendre un incident (c'est-à-dire interrompre le chronométrage de l'interruption) à la demande de SPC.

(289) Un incident suspendu par SPC doit demeurer suspendu jusqu'à ce qu'il soit relancé par SPC ou pour une période prédéterminée par SPC.

(290) 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.

(291) 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.

(292) 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.

(293) 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.

(294) L'entrepreneur doit obtenir l'autorisation de SPC avant de fermer un dossier d'incident.

(295) L'entrepreneur doit fermer les dossiers d'incident une fois que SPC en a autorisé la fermeture.

(296) L'entrepreneur doit aviser SPC de la résolution d'un incident selon la gravité de celui-ci, tel que précisé par SPC.

(297) 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.

(298) L'entrepreneur doit déterminer et consigner les facteurs de causalité (causes fondamentales) de chaque incident.

(299) L'entrepreneur doit élaborer des solutions de rechange pour toutes les causes fondamentales recensées.

(300) 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.

(301) L'entrepreneur doit hausser d'un niveau la gravité des incidents qualifiés de problèmes chroniques.

(302) L'entrepreneur doit relier les incidents aux problèmes chroniques existants ou nouveaux, à la demande de SPC.

(303) 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

(304) 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.

(305) 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.

(306) L'entrepreneur doit attendre l'approbation de SPC avant de mettre en œuvre une nouvelle version du SII.

(307) 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

(308) 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

(309) Le SII de l'entrepreneur doit réagir à toute situation de panne de manière à maintenir la disponibilité de l'accès à Internet.

(310) 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.

(311) 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.

(312) L'entrepreneur doit aviser SPC de toute interruption prévue du SII au moins vingt (20) JOGF à l'avance.

(313) L'entrepreneur doit faire approuver toute interruption prévue du SII par SPC.

6 RÉUNIONS

(314) 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.

(315) 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.

(316) 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.

(317) 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.

(318) 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.

(319) 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.

(320) L'entrepreneur doit organiser des réunions hebdomadaires et y participer afin d'examiner les DCS nouvelles ou non réglées.

(321) 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

(322) 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.

(323) L'entrepreneur doit fournir tous les rapports et autres documents concernant le SII en anglais, dans un format de fichier commercial approuvé par SPC.

(324) L'entrepreneur doit publier les rapports sur son OEIE pour que les personnes autorisées désignées par SPC puissent y accéder et les télécharger.

(325) L'entrepreneur doit assurer le suivi des versions et des modifications de tous les rapports et autres documents concernant le SII.

(326) 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.

(327) L'entrepreneur ne doit pas exiger l'utilisation de composants ActiveX pour l'accès aux rapports et aux autres documents concernant le SII.

(328) 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.

(329) 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.

(330) 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.

(331) 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.

(332) 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

(333) 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.

(334) 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.

(335) L'entrepreneur doit envoyer à SPC un rapport mensuel sur ses dépenses financières.

7.2 Rapports sur demande spéciale

(336) 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.

(337) 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.

(338) 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.

(339) 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.

(340) 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.

(341) 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

(342) 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.

(343) 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.

(344) 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.

(345) Le document de configuration sur le SII doit au moins contenir les renseignements suivants :

(345.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;

(345.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;

(345.c) la configuration de l'interface du routeur de l'entrepreneur pour le SII, sans les mots de passe;

(345.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;

(345.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;

(345.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 »);

(345.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);

(345.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.

(346) 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.

(347) L'entrepreneur doit fournir des documents à jour dans les cinq (5) JOGF concernant toute modification ou mise à jour.

(348) 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)

(349) 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.

(350) L'entrepreneur doit permettre à SPC d'utiliser cet outil dans les 60 JOGF après l'attribution du contrat.

(351) 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.

(352) L'entrepreneur doit protéger la confidentialité de l'information publiée en permettant uniquement aux personnes autorisées désignées par SPC d'y accéder.

(353) Si l'OEIE approuvé de l'entrepreneur est un portail Web ou une autre application équivalente :

(353.a) L'entrepreneur doit, sur demande, créer et gérer des comptes d'utilisateur pour les personnes désignées par SPC.

(353.b) L'OEIE doit consigner automatiquement tous les accès et l'entrepreneur doit fournir les journaux d'accès à SPC à sa demande.

(353.c) Dans l'OEIE de l'entrepreneur, les mots de passe pour la connexion des utilisateurs doivent :

(353.c.1) être composés d'au moins six caractères;

(353.c.2) être modifiés tous les 60 jours;

(353.c.3) contenir des majuscules et des minuscules et au moins un chiffre.

(353.d) L'entrepreneur doit limiter l'accès à l'OEIE par adresses IP et numéros de port d'application.

(353.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).

(354) 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.

(355) 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.

(356) L'entrepreneur doit fournir un OEIE qui permet à SPC d'exécuter, d'afficher et de télécharger des rapports.

(357) L'entrepreneur doit fournir des rapports, qui doivent être disponibles en formats HTML, XML et CSV ou dans d'autres formats approuvés par SPC.

(358) L'entrepreneur doit veiller à ce que SPC soit en mesure de personnaliser les rapports en fonction du système d'information fourni.

(359) 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.

(360) 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 5.1.

8.2 Données sur le trafic IP

(361) L'entrepreneur doit communiquer en temps réel les données sur le trafic IP sur l'OEIE.

(362) 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.

(363) 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.

(364) 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.

(365) 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

(366) L'entrepreneur doit fournir des rapports sur les méthodes de lutte contre le déni de service distribué, lesquels :

(366.a) doivent être disponibles en formats HTML, XML et CSV ou dans d'autres formats approuvés par SPC;

(366.b) doivent être automatiquement envoyés, à intervalles réguliers, aux adresses de courriel fournies par SPC;

(366.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;

(366.d) doivent indiquer les 100 adresses qui utilisent le plus de bande passante en tant que rapport sommaire Top Talker;

(366.e) doivent fournir des renseignements sur les vers informatiques et les hôtes contaminés du réseau sous forme de rapport d'activités des vers informatiques;

(366.f) doivent fournir des renseignements sur le nettoyage des données IP sur le trafic sous forme de rapport d'atténuation des menaces;

(366.g) doivent fournir des renseignements sur l'importance du trafic IP entrant, interrompu et autorisé.

8.4 Procédures de gestion des opérations

(367) Les communications entre l'entrepreneur et SPC doivent être coordonnées et transmises par l'entremise du Canada.

(368) 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.

(369) 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.

(370) 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

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

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

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

(370.a.4) Délais de résolution

(370.a.5) Analyse des causes fondamentales

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

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

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

8.4.3 Système et procédures de gestion des changements

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

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

(370.a.10) Délais d'exécution

8.4.4 Procédures de gestion de la sécurité

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

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

(370.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 :

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

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

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

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

(370.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

(371) 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.

(372) L'entrepreneur doit publier les rapports sur les niveaux de service sur son OEIE. Les rapports doivent comprendre ce qui suit :

(372.a) les valeurs relatives au rendement du service de l'entrepreneur;

(372.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;

(372.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.

(373) 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

(374) 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)

(375) 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.

(376) 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.

(377) L'entrepreneur doit fournir les renseignements suivants dans son DCI :

(377.a) ses coordonnées;

(377.b) une description de la couche physique du SII;

(377.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.

(378) L'entrepreneur doit s'assurer que les renseignements qu'il inscrit dans le DCI sont exacts et à jour.

(379) L'entrepreneur doit apporter les modifications ou les mises à jour qui s'imposent dans le DCI dans les trois (3) JOGF.

(380) L'entrepreneur doit émettre le DCI révisé et le présenter à SPC après révision.

8.9 Sécurité

(381) 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.

(382) 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.

(383) 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.

(384) 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.

(385) 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 :

(386) 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.

(387) 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

(388) Chaque année, SPC peut procéder à un examen de la conformité qui comprend, entre autres, les éléments suivants :

a) veiller à ce que le SII soit conforme aux exigences relatives à la sécurité;

b) 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;

c) 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;

d) s'assurer que l'entrepreneur examine quotidiennement les journaux de vérification de la sécurité.

(389) 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.

(390) 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

(391) 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.

(392) 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.

(393) 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.

(394) L'entrepreneur doit surveiller et mesurer les niveaux de service, 24 heures sur 24, tous les jours de l'année.

(395) L'entrepreneur doit fournir tout matériel et logiciel nécessaire à la surveillance et à la mesure des niveaux de service.

(396) 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.

(397) 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.

(398) 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.

(399) 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 :

$$\frac{\textit{(Disponibilité du service attendue pour le mois - temps d'interruption durant le mois)}}{\textit{disponibilité du service attendue pour le mois}} \times 100\ \%$$

(400) 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)

(401) 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)

(402) 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).

(403) 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.

(404) 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)

(405) Le NS-DMRS du SII et le service anti-déni de service distribué est de quatre (4) heures.

(406) 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.

(407) 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)

(408) 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	▪ 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.	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.
Délai de transit des paquets (NS – DT)	▪ 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.	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. 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.

Tableau 7 – Niveaux de service du SII

Paramètre du niveau de service	Descriptions	Exigence du niveau de service
Perte de paquets de données (NS – PP)	▪ 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.	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.
Disponibilité	▪ 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.	▪ **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)