Énoncé des travaux (ET) Annexe A - Appendice B, Contrôles de sécurité des SII

Le présent appendice porte sur les exigences relatives aux contrôles de sécurité des services d'interconnexion Internet (SII) qui ont été sélectionnés dans le document intitulé « Conseils en matière de sécurité des technologies de l'information - La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie - Catalogue des contrôles de sécurité - ITSG-33 – Annexe 3 » (http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg33-ann3-fra.html). L'entrepreneur doit consulter l'ITSG-33 – Annexe 3 pour obtenir une description complète des contrôles et des améliorations de contrôle.

Remarques :

a) L'abréviation DSP correspond à demande de soumissions provisoire qui a été transmise pendant le processus de demande de réponses pour l'évaluation (DRPE).
b) L'abréviation ET renvoie à énoncé des travaux qui accompagne la DRPE.
c) Les références aux clauses qui figurent dans la demande de soumissions et l'ET s'ajoutent au profil personnalisé ITSG-33 Protégé A / Assurance moyenne / Disponibilité moyenne (Protégé A / Intégrité faible / Disponibilité faible).
d) Le présent profil ne contient pas toutes les clauses de sécurité de la demande de soumissions et de l'ET. Pour les clauses qui apparaissent dans la demande de soumissions ou l'ET, on renvoie à l'en-tête et au paragraphe du document.
e) La matrice de traçabilité des exigences de sécurité (MTES) doit montrer la conformité aux clauses de sécurité de la demande de soumissions et de l'ET ainsi qu'aux exigences citées dans le présent profil de contrôle.
f) Le sigle OEIE renvoie à « Outil d’échange d’information électronique ».

N° de MTES	Famille	Identification de contrôle Amélioration	Nom	Clauses des SII et contrôles supplémentaires de l'ITSG-33 pour l'évaluation et l'autorisation de sécurité
SRTM 1	AC	2	GESTION DES COMPTES	L'entrepreneur doit gérer les comptes des utilisateurs de l'infrastructure de service de la solution de SII de la manière suivante : a) désigner les types de comptes (de personne, de groupe, de système, d'appareil, d'application, client ou anonyme et temporaire); b) établir les conditions d'appartenance à un groupe; c) désigner les utilisateurs autorisés de l'infrastructure de service de la solution de SII et préciser les privilèges d'accès; d) exiger les approbations nécessaires lors du traitement des demandes de création de comptes; e) choisir un identificateur qui désigne de manière unique l'utilisateur ou l'appareil; f) attribuer l'identificateur de l'utilisateur à la personne ou au groupe auquel il est destiné ou l'identificateur d'appareil au dispositif auquel il est destiné; g) établir, activer, modifier, désactiver et supprimer des comptes; h) autoriser et surveiller plus particulièrement l'utilisation des comptes clients, anonymes et temporaires; i) informer le gestionnaire de comptes lorsque des comptes temporaires ne sont plus requis et que des comptes d'exploitants autorisés de l'infrastructure de service de la solution de SII sont fermés, transférés, ou que des changements ont été apportés à l'utilisation de l'infrastructure de service de la solution de SII ou, au besoin, de connaître ou d'échanger l'information; j) empêcher la réutilisation des identificateurs pendant au moins un an; k) désactiver : i) les comptes temporaires qui ne sont plus nécessaires; ii) les comptes des utilisateurs qui ont quitté leur emploi ou qui ont été transférés; iii) les comptes qui sont demeurés inactifs pendant un certain nombre de jours précisé par SPC; iv) les comptes temporaires et créés en cas d'urgence ayant dépassé un certain âge;

					l) accorder l'accès à l'infrastructure de service SII en tenant compte des points suivants : i) une autorisation d'accès valide a été obtenue; ii) l'utilisation du système prévu; iii) le respect des autres exigences de l'entrepreneur ou de SPC; m) examiner les comptes au moins une fois par mois; n) procéder au verrouillage du compte après 10 tentatives infructueuses entreprises dans un délai de 5 minutes; o) maintenir le compte verrouillé jusqu'à ce qu'un autre utilisateur le déverrouille manuellement.
SRTM 2	AC	2	(2)	GESTION DES COMPTES	L'entrepreneur doit fermer et désactiver les comptes temporaires et d'urgence utilisés dans la gestion, la résolution des incidents ou le dépannage des composants du système des SSI : A) dans les 48 heures suivant la résolution des incidents nécessitant la création d'un compte, ou B) après une semaine d'inactivité.
SRTM 3	AC	2	(4)	GESTION DES COMPTES	L'OEIE, le système de vérification des SII et tous les composants des SII déployés à un point d'interface de service (PIS) du gouvernement du Canada vérifient automatiquement la création, la modification, la désactivation et la fermeture des comptes privilégiés et informe, au besoin, les personnes compétentes.
SRTM 4	AC	3		APPLICATION DE L'ACCÈS	L'infrastructure de service des SII de SPC doit appliquer les autorisations d'accès pour les utilisateurs.

SRTM 5	AC	4	APPLICATION DES CONTRÔLES DU FLUX D'INFORMATION	L'entrepreneur doit obtenir une autorisation de SPC avant la mise en œuvre et l'utilisation du contrôle du flux de l'information ou des dispositifs de modification du flux dans le service des SII, comme entre autres : A) les pare-feux, B) les mandataires d'application; C) les dispositifs de mise en cache des pages Web ou du contenu; D) la prévention de la perte de données; E) la compression des données ou du contenu; F) la priorité du service; G) la qualité du service; H) l'inspection des médias sociaux ou la mise en cache du contenu; I) la substitution du contenu (p. ex., publicités ciblées); J) la technologie relative au réacheminement vers le site. [DRPE EDT 2.1, paragraphe (36)] L'entrepreneur doit s'assurer que le trafic IP n'est pas intégré dans ce service. [DSP 7.7.6.4] L'entrepreneur doit s'assurer que le trafic sur le réseau national (c'est-à-dire le trafic partant d'une partie du Canada vers une destination située dans une autre partie du Canada) s'effectue exclusivement au Canada.
SRTM 6	AC	5	SÉPARATION DES TÂCHES	L'entrepreneur doit veiller à la séparation des tâches des utilisateurs, si nécessaire, afin de prévenir toute activité malveillante et toute collusion en fonction du profil d'accès accordé à l'utilisateur selon son rôle.

SRTM 7	AC	6	DROIT D'ACCÈS MINIMAL	L'entrepreneur doit mettre en œuvre une politique de privilège minimum à l'égard des utilisateurs de l'infrastructure des SII de la manière suivante : a) configurer les mécanismes de contrôle d'accès de manière à accorder le privilège minimum, soit en ne donnant aux utilisateurs (et aux processus exécutés en leur nom) que l'accès dont ils ont besoin pour accomplir les tâches qui leur sont attribuées; b) créer des comptes non privilégiés qui seront utilisés pour les tâches non opérationnelles; c) limiter l'attribution de comptes super-utilisateur (p. ex. racine) aux utilisateurs désignés; d) limiter le partage des comptes d'utilisateur; e) identifier de manière distincte l'utilisateur qui a effectué chaque intervention sur l'infrastructure de service de la solution de SII. [DSP 7.7.7.1.1] [L'entrepreneur doit] contrôler les accès à toutes les bases de données relatives au présent contrat, de manière à limiter ces accès aux personnes le nécessitant pour exécuter le contrat et ayant les attestations de sécurité au niveau stipulé au contrat; [DSP 7.7.7.1.2] [L'entrepreneur doit] faire en sorte que les mots de passe ou les autres contrôles d'accès ne soient fournis qu'aux personnes qui en ont besoin pour exécuter les travaux et qui détiennent une attestation de sécurité émise par la Direction de la sécurité industrielle canadienne (DSIC) au niveau exigé par le contrat;
SRTM 8	AC	8	NOTIFICATION D'UTILISATION SYSTÈME	L'infrastructure des SII déployée à un PIS doit, avant d'accorder l'accès au système, afficher un message ou une bannière de notification d'utilisation approuvée du système qui comprend des énoncés de confidentialité et de sécurité conformément à la Politique d'utilisation des réseaux électroniques du Secrétariat du Conseil du Trésor (SCT). Le message ou la bannière d'avis doit rester sur l'écran jusqu'à ce que l'utilisateur prenne des mesures explicites pour ouvrir une session ou accéder au composant des SII.

SRTM 9	AC	17		ACCÈS À DISTANCE	[EDT 5, paragraphe (245)] (237) Afin de gérer et d'administrer à distance les services de gestion associés aux SII, l'entrepreneur doit 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. [DSP 7.7.8.1] L'entrepreneur doit s'assurer que l'équipement ou tous les composants qui font partie du système utilisé pour assurer la prestation des services de réseau peuvent être gérés au moyen de protocoles sécurisés. [DSP 7.7.8.2] Si l'entrepreneur utilise des serveurs de gestion dont le niveau de sécurité ou le chiffrement peut être configuré, il doit désactiver tous les niveaux autres que le niveau de sécurité ou le chiffrement le plus élevé. [DSP 7.7.8.3] L'entrepreneur ne doit pas utiliser des protocoles selon lesquels les noms d'utilisateur et les mots de passe sont transmis en clair dans le réseau. [DSP 7.7.8.4] L'entrepreneur ne doit pas utiliser de protocoles (et doit les désactiver) qui ne peuvent pas passer par des coupe-feux compatibles avec la session. [DSP 7.7.8.5] Le Canada ne considérera pas qu'un protocole non sécurisé est sécurisé au moyen de techniques de tunnellisation, comme le réacheminement de port ou IPSec. [DSP 7.7.8.6] L'entrepreneur doit mettre en œuvre les protocoles de chiffrement relevés par le Canada et désactiver tous les protocoles de chiffrement qui ne sont pas approuvés par celui-ci.
SRTM 10	AC	17	(5)	ACCÈS À DISTANCE	L'entrepreneur doit surveiller les connexions à distance non autorisées aux composants de SII déployés à un PIS du gouvernement du Canada et prendre des mesures adéquates si une connexion non autorisée est constatée.
SRTM 11	AC	22		CONTENU ACCESSIBLE AU PUBLIC	L'entrepreneur des SII doit obtenir une autorisation de SPC avant d'afficher de l'information, y compris des statistiques, liée au Canada, transmise par celui-ci ou inférée dans la mission contractuelle avec le Canada.

SRTM 12	AU	2	ÉVÉNEMENTS VÉRIFIABLES	L'entrepreneur doit s'assurer que l'OEIE, le système de vérification des SII et les composants des SII déployés à un PIS du gouvernement du Canada vérifient au moins les événements d'utilisateur ou de processus privilégiés suivants : a) Tentatives fructueuses et infructueuses d'accès, de modification ou de suppression d'objets de sécurité (ces objets incluent les données de vérification, les fichiers de configuration de système et les permissions d'accès formelles de fichier et d'utilisateur) b) Tentatives fructueuses et infructueuses de connexion c) Activités privilégiées ou autre accès au niveau du système d) Heure de début et de fin de l'accès de l'utilisateur au système e) Tous les lancements de programme De plus, le système d'information vérifie au moins les événements d'utilisateur ou de processus non privilégiés suivants : a) Tentatives fructueuses et infructueuses d'accès, de modification ou de suppression d'objets de sécurité b) Tentatives fructueuses et infructueuses de connexion d) Heure de début et de fin de l'accès de l'utilisateur au système

SRTM 13	AU	3	CONTENU DES ENREGISTREMENTS DE VÉRIFICATION	L'entrepreneur des SII doit veiller à ce que les composants du système des SII génèrent des enregistrements de vérification permettant, au minimum, d'établir le type d'événement survenu, la date et l'heure, la nature de l'événement, l'endroit où il s'est produit, sa source, son résultat (succès ou échec) ainsi que l'identité de tout utilisateur ou sujet associé à l'événement. [DSP 7.7.7.3] L'entrepreneur doit conserver un registre de vérification qui enregistre automatiquement toutes les tentatives d'accès au réseau du Canada, ainsi qu'à toutes les bases de données qui comprennent les données ou des renseignements sur le Canada conservés par l'entrepreneur (comme des renseignements sur la facturation et des renseignements détaillés sur les appels). Chaque action, transaction ou fonction opérationnelle exécutée sur le réseau, les systèmes ou les bases de données de l'entrepreneur liés au contrat doit pouvoir être retracée jusqu'à un utilisateur ou un compte individuel (en s'assurant que les identificateurs et les comptes des utilisateurs sont uniques et qu'ils ne peuvent pas être partagés ou transférés d'une personne à une autre).
SRTM 14	AU	4	CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS	L'entrepreneur des SII ne doit pas annuler d'événement de vérification pour accroître la capacité de stockage.

SRTM 15	AU	5	INTERVENTION EN CAS D'ÉCHEC DE VÉRIFICATION	L'entrepreneur doit s'assurer qu'en cas d'échec de vérification dans l'OEIE, le système de vérification des SII ou les composants des SII déployés à un PIS du gouvernement du Canada, les agents désignés de l'organisation de l'entrepreneur sont alertés et que ces anomalies sont indiquées dans les rapports fournis par l'OEIE.

SRTM 16	AU	6	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	L'entrepreneur des SII doit examiner et analyser les enregistrements de vérification de sécurité du composant PIS des SII pour voir s'il y a des activités inadéquates ou inhabituelles et transmettre ses conclusions aux agents du Centre de coordination de la sécurité de la TI de SPC. L'entrepreneur doit adapter le niveau d'examen, d'analyse et de rapport des vérifications en cas de changement relatif aux risques liés à ses activités, aux actifs, aux personnes, aux autres organisations, ou au Canada, selon l'information relative à l'application de la loi, découlant du renseignement ou provenant d'autres sources crédibles.

SRTM 17	AU	6	(1)	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	L'entrepreneur doit adapter le niveau d'examen, d'analyse et de rapport des vérifications dans le système d'information en cas de changement relatif aux risques liés à ses activités, aux actifs, aux personnes, aux autres organisations, ou au Canada, selon l'information relative à l'application de la loi, découlant du renseignement ou provenant d'autres sources crédibles.

SRTM 18	AU	8	ESTAMPILLES TEMPORELLES	L'entrepreneur des SII doit s'assurer que les composants des SII synchronisent les horloges de système internes en utilisant une source temporelle faisant autorité et approuvée par SPC afin de générer des estampilles temporelles pour les enregistrements de vérification.

SRTM 19	AU	9	(4)	PROTECTION DE L'INFORMATION DE VÉRIFICATION	L'entrepreneur doit restreindre l'accès à la gestion de la fonctionnalité de vérification des SII à un sous-groupe limité d'utilisateurs privilégiés.
SRTM 20	AU	11		CONSERVATION DES ENREGISTREMENTS DE VÉRIFICATION	[EDT 8.9, paragraphe (383)] L'entrepreneur doit conserver les enregistrements sur les violations de la sécurité, les transactions et les vérifications, ainsi que sur les rapports d'incident d'alarme et les rapports connexes de l'année en cours et des deux années précédentes, et obtenir l'autorisation écrite de SPC avant de détruire tout rapport datant de plus de deux ans.

SRTM 21	CA	2	ÉVALUATIONS DE SÉCURITÉ	[EDT 3.6.6, paragraphe (157) L'entrepreneur doit présenter à SPC un rapport sur l'architecture de sécurité qui décrit son infrastructure, c'est-à-dire : 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.

SRTM 22	CA	5	(1)	PLAN DE MISE EN ŒUVRE DES MESURES DE PROTECTION (PLAN D'ACTION ET JALONS)	[EDT 3.6.5, paragraphe (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.
SRTM 23	CM	2		CONFIGURATION DE RÉFÉRENCE	[EDT, paragraphe 5.2 (270)] L'entrepreneur doit s'acquitter des tâches suivantes de gestion de la configuration pour les 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 des SII, conformément aux exigences du Canada; 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 le Canada en fait la demande, en respectant la convention d'appellation de fichier précisée par le Canada 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).
SRTM 24	CM	2	(5)	CONFIGURATION DE RÉFÉRENCE	L'entrepreneur des SII doit créer, tenir à jour, restreindre et contrôler la liste des applications, des programmes logiciels et des processus dont l'exécution est autorisée sur l'OEIE.

SRTM 25	CM	6		PARAMÈTRES DE CONFIGURATION	[EDT 8.1, paragraphe (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-feux et de routeurs filtrant les adresses IP. (353.d) L'entrepreneur doit limiter l'accès à l'OEIE par adresses IP et numéros de port d'application. [DSP 7.7.7.3] À moins que le responsable technique ne le demande, l'entrepreneur doit désactiver les ports d'écoute TCP/UDP pour tout l'équipement déployé dans le réseau du Canada ou dans l'infrastructure de réseau ou le réseau de base de l'entrepreneur qui est interconnecté au réseau du Canada. Des méthodes de contrôle d'accès strictes doivent être en place pour tous les ports ouverts aux fins de gestion du réseau.
SRTM 26	CM	7		FONCTIONNALITÉ MINIMALE	L'entrepreneur doit appliquer et mettre en œuvre un principe de privilège restreint pour les composants du système de SII et l'OEIE.
SRTM 27	CM	8		INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	[EDT 7.2, paragraphe (338)] L'entrepreneur est tenu de fournir au Canada, sur demande spéciale, un rapport d'inventaire spécial décrivant l'équipement dont sont dotés les emplacements en ce qui concerne les 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.
SRTM 28	CM	8	1)	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	L'entrepreneur doit mettre à jour l'inventaire des composants du système d'information déployés à un PIS du gouvernement du Canada dans le cadre des activités d'installation et de retrait des composants et de mise à jour du système d'information.

SRTM 29	CP	1		POLITIQUE ET PROCÉDURES DE PLANIFICATION D'URGENCE	[EDT 3.3, paragraphe (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 principaux composants 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 le Canada peut s'attendre à ce que les services soient rétablis.
SRTM 30	CP	2		PLAN D'URGENCE	[EDT 5.6, paragraphe (309)] Le SII de l'entrepreneur doit réagir à toute situation de panne de manière à maintenir la disponibilité de l'accès à Internet. [EDT 5.6, paragraphe (310)] L'entrepreneur doit s'acquitter des tâches de gestion de la disponibilité suivante : 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;
SRTM 31	IA	2		IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	L'OEIE doit appliquer l'authentification à deux facteurs à l'aide du jeton cryptographique matériel pour tous les comptes d'utilisateur autorisés conformément à l'ITSG-31 du Centre de la sécurité des télécommunications Canada (CSTC), section 2.2.1.3, niveau 3. L'entrepreneur doit appliquer l'authentification à deux facteurs pour la gestion intrabande des composants des SII déployés à un PIS du gouvernement du Canada.
SRTM 32	IA	2	(100)	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	En ce qui concerne l'accès à distance aux comptes privilégiés, les composants du système de SII déployés à un PIS du gouvernement du Canada nécessitent une authentification multifactorielle.

SRTM 33	IA	4	GESTION DES IDENTIFICATEURS	L'entrepreneur des SII doit gérer les identificateurs des utilisateurs et des dispositifs utilisés dans la gestion ou l'exploitation de l'infrastructure des SII et des composants en : a) recevant l'autorisation d'une autorité responsable désignée d'attribuer un identificateur d'utilisateur ou de dispositif; b) sélectionnant un identificateur qui identifie de façon unique l'utilisateur ou le dispositif; c) attribuant l'identificateur d'utilisateur à la personne prévue ou l'identificateur du dispositif au dispositif concerné; d) empêchant la réutilisation de l'identificateur d'utilisateur ou de dispositif pendant 180 jours; e) désactivant l'identificateur d'utilisateur après 30 minutes d'inactivité. L'entrepreneur ne doit pas, pour gérer l'infrastructure ou les composants des SII, utiliser des identificateurs de compte du système qui mettent également les comptes en correspondance selon des méthodes de reconnaissance (c'est-à-dire l'obtention de coordonnées accessibles au public), p. ex., par l'intermédiaire du contact DNS, des sites de médias sociaux ou d'une autre association technique avec l'entrepreneur)
SRTM 34	IA	5	GESTION DES AUTHENTIFICATEURS	L'entrepreneur des SII doit gérer les authentificateurs des utilisateurs et des dispositifs en : a) vérifiant l'identité de la personne ou du dispositif, au moment de l'attribution initiale des authentificateurs; b) établissant le contenu initial des authentificateurs définis par l'entrepreneur; c) veillant à ce que les authentificateurs soient suffisamment robustes pour l'utilisation prévue; d) établissant et en mettant en application des procédures administratives concernant la distribution initiale des authentificateurs, les authentificateurs perdus, endommagés ou compromis, et l'annulation des authentificateurs; e) modifiant le contenu par défaut des authentificateurs au moment de l'installation du système d'information; f) établissant les conditions minimales et maximales d'utilisation à vie et les conditions de réutilisation des authentificateurs (le cas échéant); g) modifiant ou actualisant les authentificateurs par mot de passe au moins tous les 180 jours; h) protégeant le contenu des authentificateurs contre la divulgation et la modification non autorisées; i) exigeant des utilisateurs et des dispositifs qu'ils appliquent des mesures spécifiques de protection des authentificateurs.

SRTM 35	IA	5	1)	GESTION DES AUTHENTIFICATEURS	L'authentificateur par mot de passe permettant d'accéder à l'OEIE doit : [EDT 8.1, paragraphe (353.c.1)] être composé d'au moins six caractères; [EDT 8.1, paragraphe (353.c.2)] être modifié tous les 60 jours; [EDT 8.1, paragraphe (353.c.3)] contenir des majuscules et des minuscules et au moins un chiffre.
SRTM 36	IA	6		RÉTROACTION D'AUTHENTIFICATION	L'OEIE doit rendre illisibles les rétroactions d'authentification durant le processus d'authentification afin de protéger l'information contre de possibles exploitations ou utilisations par des personnes non autorisées.
SRTM 37	IR	5		SURVEILLANCE DES INCIDENTS	[EDT 4.4, paragraphe (226)] L'entrepreneur doit surveiller et signaler tous les incidents 24 heures sur 24, tous les jours de l'année concernant les services fournis au Canada.
SRTM 38	IR	6		SIGNALEMENT DES INCIDENTS	[EDT 3.6.8, paragraphe (159)] L'entrepreneur doit fournir des avis et générer des billets sur les incidents relatifs à la sécurité qui comprennent entre autres les renseignements suivants : a) le genre et la description d'une attaque; b) la possibilité que l'attaque ait réussi, 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. [DSP 7.7.9.1] L'entrepreneur doit fournir au responsable technique des renseignements opportuns sur les vulnérabilités (c.-à-d. les faiblesses ou les lacunes de conception cernées dans l'équipement fourni selon le contrat/tout composant du système utilisé pour fournir les services du réseau qui permettraient à une personne non autorisée de compromettre l'intégrité, la confidentialité, les contrôles d'accès, la disponibilité, la cohérence ou le mécanisme de vérification du système ou des données et applications qu'il héberge).
SRTM 39	MP	1		POLITIQUE ET PROCÉDURES DE PROTECTION DES SUPPORTS	L'entrepreneur doit, pendant la phase de préparation opérationnelle, développer et diffuser une politique de protection et de traitement des supports portant sur les rôles, les responsabilités, les restrictions ainsi que la conformité au traitement des supports contenant les journaux du gouvernement du Canada liés à la fourniture des SII, y compris : A) l'accès physique et logique aux journaux et aux supports de données des SII, y compris les dispositifs temporaires ou portatifs utilisés pour le transfert ou l'analyse des journaux des SII; B) les processus et procédures de destruction pour les supports servant à enregistrer ou à traiter les journaux du gouvernement du Canada;

				C) la transmission des supports ou des journaux aux responsables autorisés du gouvernement du Canada; D) les exigences de protection des données en vue de l'inclusion des journaux du gouvernement du Canada (protégés A) lors des communications avec le gouvernement du Canada (hormis l'OEIE).
SRTM 40	MP	2	ACCÈS AUX SUPPORTS	L'entrepreneur doit mettre en œuvre des mesures de contrôle d'accès pour s'assurer que seules les personnes autorisées peuvent accéder aux supports contenant les journaux des SII, les rapports d'incident, les habitudes d'utilisation et les statistiques.
SRTM 41	MP	3	MARQUAGE DES SUPPORTS	L'entrepreneur doit : a) indiquer clairement, sur les supports amovibles et les sorties du système d'information contenant ou affichant l'information protégée du Canada, les limites de distribution, les mises en garde concernant le traitement, et les mentions de sécurité (le cas échéant) de l'information; b) contrôler physiquement et entreposer de manière sécurisée les supports numériques et non numériques contenant l'information protégée du Canada conformément au document G1-00, Guide d'équipement de sécurité de la Gendarmerie royale du Canada (GRC); c) protéger physiquement et entreposer de manière sécurisée les supports de système d'information protégée en attente de leur destruction (sur place ou à l'extérieur) en utilisant de l'équipement, des techniques et des procédures approuvés.
SRTM 42	MP	6	NETTOYAGE DES SUPPORTS	a) L'entrepreneur doit nettoyer les supports de données informatiques contenant des données protégées du Canada, qu'ils soient sous forme numérique et non numérique, avant de les éliminer, de les soustraire au contrôle du fournisseur, ou de les rendre accessibles aux fins de réutilisation. b) L'entrepreneur doit utiliser des mécanismes de nettoyage approuvés par le Canada; c) L'entrepreneur doit suivre, documenter et vérifier le nettoyage des supports et les activités d'élimination.

SRTM 43	PE	2		AUTORISATION D'ACCÈS PHYSIQUE	L'entrepreneur doit mettre en œuvre, en fonction du rôle des employés, un contrôle d'accès physique aux installations de l'infrastructure de service des SII où se trouvent l'OEIE et le système de vérification contenant les journaux des SII, y compris : a) tenir une liste du personnel autorisé à accéder aux installations; b) émettre des justificatifs d'autorisation d'accès aux installations; c) examiner et approuver la liste d'accès et les justificatifs d'autorisation à tout moment au moins tous les mois, en retirant de la liste d'accès le nom des membres du personnel qui n'ont plus besoin d'accéder aux installations; d) autoriser l'accès physique aux installations, par point d'accès, en fonction du rôle de la personne; e) modifier l'attribution du rôle lorsque l'utilisateur assume un nouveau rôle; f) assurer la séparation des tâches lorsque l'autorisation d'accéder aux installations est accordée par une autre personne que celle qui autorise l'accès à l'infrastructure de service des SII; g) permettre au personnel autorisé d'accéder aux installations en fonction de leur besoin de savoir ou leur besoin d'accès; [DSP 7.7.1] L'entrepreneur et ses employés doivent TOUS avoir une cote de fiabilité valide délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.
SRTM 44	PE	2	(100)	AUTORISATIONS D'ACCÈS PHYSIQUE	[DSP 7.7.3.3] Dès leur arrivée dans les installations du Canada, tous les employés de l'entrepreneur et du sous-traitant approuvés au préalable par l'autorité contractante doivent être en mesure de fournir une preuve d'emploi (comme un insigne émis par l'entrepreneur ou par le sous-traitant approuvé), et le statut de leur attestation de sécurité doit être validé par une source sûre. L'entrepreneur doit remettre une carte d'identification à tous les employés qui remplissent une fonction ou ont des responsabilités concernant le service des SII. Cette carte doit comprendre au moins le nom de l'organisation, le nom et la photo du détenteur de la carte, un numéro de carte unique et une date d'expiration. Pour autoriser l'accès physique aux installations où se trouvent l'OEIE et le système de vérification, l'entrepreneur doit exiger que cette carte d'identification soit présentée.

SRTM 45	PE	3	CONTRÔLE D'ACCÈS PHYSIQUE	L'entrepreneur du SII doit : a) faire respecter les autorisations d'accès physiques à tous les points d'accès physiques (y compris les entrées et sorties désignées) des installations où est située l'infrastructure des SII (à l'exclusion des zones à l'intérieur des installations qui sont officiellement désignées comme étant accessibles au public); b) vérifier les autorisations d'accès individuelles avant d'accorder l'accès aux installations; c) contrôler les entrées de l'installation qui héberge le système d'information en recourant à des dispositifs de contrôle d'accès physique ou à des agents de sécurité; d) contrôler l'accès aux zones officiellement désignées comme étant accessibles au public conformément à l'évaluation des risques effectuée par l'organisation; e) garder les clés, les combinaisons et les autres dispositifs de contrôle de l'accès physique en lieu sûr; f) faire l'inventaire exact des dispositifs de contrôle de l'accès physique; g) modifier les combinaisons et les clés lorsque des clés sont perdues, lorsque des combinaisons sont compromises ou lorsque des employés sont transférés ou quittent leur poste. [DRPE 2.3.1, DSP 7.7.1] L'entrepreneur doit posséder une autorisation de détenir des renseignements (ADR) au niveau « protégé A » délivrée par le Programme de sécurité industrielle de Travaux publics et Services gouvernementaux Canada.
SRTM 46	PE	6	SURVEILLANCE DE L'ACCÈS PHYSIQUE	L'entrepreneur du SII doit : a) surveiller l'accès physique à l'OEIE et aux systèmes de vérification des SII afin de détecter les incidents de sécurité physique et d'y répondre; b) examiner les journaux d'accès physique tous les mois et après des incidents suspectés; c) coordonner les résultats des examens et des enquêtes avec sa capacité d'intervention en cas d'incident.
SRTM 47	PE	16	LIVRAISON ET RETRAIT	L'entrepreneur des SII doit autoriser, surveiller et contrôler l'entreposage et le traitement des composants de l'infrastructure des SII qui entrent dans les installations et tenir à jour les dossiers de ces composants afin d'appuyer les objectifs d'intégrité de la chaîne d'approvisionnement. [DSP 7.7.1] L'entrepreneur ou son personnel NE DOIT PAS emporter hors des établissements de travail visés des renseignements ou des biens CLASSIFIÉS ou

					PROTÉGÉS B et C.
SRTM 48	PL	2		PLAN DE SÉCURITÉ DU SYSTÈME	A) L'entrepreneur des SII doit développer pour les SII, l'OEIE et le système de vérification des SII, un plan de sécurité qui : i) décrit l'environnement opérationnel; ii) décrit les relations ou les connexions avec d'autres entrepreneurs des SII ou fournisseurs en amont; iii) donne un aperçu des exigences en matière de contrôle de sécurité pour les SII, l'OEIE et le système de vérification des SII; iv) décrit les contrôles de sécurité existants ou prévus pour répondre à ces exigences (ainsi que les exigences incluses dans le présent profil de contrôle), y compris la justification des décisions concernant l'adaptation des contrôles et l'application de conseils supplémentaires; v) est examiné et approuvé par le responsable de SPC avant sa mise en œuvre. B) L'entrepreneur des SII doit examiner chaque année le plan de sécurité du système d'information. C) L'entrepreneur des SII doit mettre le plan à jour pour tenir compte des changements apportés au système des SII ou à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en œuvre du plan ou des évaluations des contrôles de sécurité.
SRTM 49	PL	2	(1)	PLAN DE SÉCURITÉ DU SYSTÈME	[EDT 3.6.4, paragraphe (155)] L'entrepreneur doit présenter au Canada 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.

SRTM 50	PL	2	(2)	PLAN DE SÉCURITÉ DU SYSTÈME	[EDT 3.6.6, paragraphe (157) L'entrepreneur doit présenter au Canada 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 documents ITSG-22 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-fra.pdf] et ITSG-38 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-fra.pdf] du 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 des SII en interaction directe et indirecte avec l'infrastructure du gouvernement du Canada (p. ex., des routeurs) doit avoir été préalablement validé en vertu d'un système de critères communs reconnu, en le comparant à un profil de protection, ou en l'absence de ce dernier, à une cible de sécurité applicable dont les exigences en matière d'assurance sont conformes à la certification EAL-2 ou aux dispositions contenues dans une documentation approuvée en matière d'assurance; e) pour chiffrer les communications entre le gouvernement du Canada et l'entrepreneur, les modules cryptographiques servant à accéder à l'OEIE doivent être validés conformes à la norme FIPS 140-2 ou à des normes 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.
SRTM 51	PS	3		ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL	[EDT 8.4, paragraphe (370.a.13)] (...) chacun des employés de l'entrepreneur, et toute personne ou tout 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.

SRTM 52	PS	4		CESSATION D'EMPLOI	a) L'entrepreneur, lors de la cessation d'emploi d'un employé, doit mettre un terme à son accès logique et physique à l'infrastructure et aux composants des SII. b) L'entrepreneur, lors de la cessation d'emploi d'un employé, doit lui retirer tous les biens et toute l'information liés à la sécurité des SII.
SRTM 53	SA	3		SOUTIEN DU CYCLE DE VIE	A) L'entrepreneur doit gérer l'OEIE et les systèmes de vérification des SII en utilisant une méthodologie de cycle de développement des systèmes qui inclut les aspects liés à la sécurité de l'information. B) L'entrepreneur doit déterminer et documenter les rôles et les responsabilités à tous les stades du cycle de développement du système. C) L'entrepreneur doit identifier les personnes auxquelles sont attribués des rôles et des responsabilités associés à la sécurité du système d'information.
SRTM 54	SA	4	(7)	ACQUISITIONS	[EDT 3.6.6, paragraphe (157)] d) L'équipement qu'utilise l'entrepreneur pour assurer la prestation des SII en interaction directe et indirecte avec l'infrastructure du gouvernement du Canada (p. ex. des routeurs) doit avoir été préalablement validé en vertu d'un système de critères communs reconnu, en le comparant à un profil de protection approuvé, 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.
SRTM 55	SA	5		DOCUMENTATION DES SYSTÈMES D'INFORMATION	A) L'entrepreneur doit obtenir, protéger s'il y a lieu, et mettre à la disposition du personnel autorisé et du Canada, sur demande, pour l'OEIE, le système de vérification des SII et les composants des SII déployés à un PIS du gouvernement du Canada, une documentation de l'administrateur décrivant : i) la configuration, l'installation et l'exploitation sécurisées du système d'information; ii) l'utilisation et la maintenance efficaces des options et des fonctions de sécurité; iii) les vulnérabilités connues en ce qui concerne la configuration et l'utilisation des fonctions d'administration (fonctions privilégiées). B) L'organisation obtient, protège s'il y a lieu, et communique au personnel autorisé la documentation destinée aux utilisateurs du système d'information et décrivant : i) les options et fonctions de sécurité accessibles aux utilisateurs et leur utilisation efficace; ii) les méthodes d'interaction entre les utilisateurs et le système d'information, ce qui permet aux personnes d'utiliser le système de manière plus sécurisée; iii) les responsabilités des utilisateurs à l'égard de la sécurité des données et du système d'information. C) L'organisation documente les tentatives d'obtenir des documents sur le système

					d'information qui n'existent pas ou qui ne sont pas disponibles.
SRTM 56	SA	12	(2)	PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT	[DSP 7.8.1] À tout moment durant la période du contrat, si l'entrepreneur propose d'introduire de nouveaux produits commerciaux qui ne font pas partie de la liste des produits de TI approuvés par le Canada, dans le réseau du Canada, dans l'infrastructure de l'entrepreneur ou son réseau de base, ou dans ceux de la tierce partie, produits qui seront interconnectés avec le réseau du Canada, l'entrepreneur doit obtenir au préalable l'approbation écrite du responsable technique. Le Canada se réserve le droit de refuser de nouveaux produits commerciaux, de proposer de nouvelles mesures de protection, de valider de façon indépendante et d'approuver les produits commerciaux. [DSP 7.8.2] À tout moment, si le Canada avise l'entrepreneur qu'un fabricant ou un fabricant original de matériel (OEM) n'est plus considéré comme un fabricant ou un OEM de confiance (c.-à-d. un fabricant en qui on ne fait plus confiance), l'entrepreneur (et ses sous-traitants) doit immédiatement cesser de déployer l'équipement manufacturé par le fabricant ou l'OEM dans le réseau du Canada et dans toute infrastructure ou réseau de base de l'entrepreneur qui se raccordera au réseau du Canada. Pour ce qui est de l'équipement déjà déployé, l'entrepreneur doit identifier ou enlever l'équipement manufacturé par ce fabricant ou cet OEM qui serait dans le réseau du Canada et dans toute infrastructure ou réseau de base de l'entrepreneur qui se raccordera au réseau du Canada. Si le Canada demande un changement en vertu de cette section, l'entrepreneur aura droit à un ajustement équitable. [DSP 7.8.3] Si l'entrepreneur est informé qu'un tiers (sauf un sous-traitant) déploie un équipement non éprouvé sur son réseau, il doit immédiatement en informer le responsable technique.
SRTM 57	SC	2		PARTITIONNEMENT DES APPLICATIONS	L'entrepreneur des SII doit prendre des mesures physiques ou logiques pour assurer le partitionnement de la fonctionnalité utilisateur (y compris des services d'interface utilisateur) de la fonctionnalité de gestion de l'OEIE, du système de vérification des SII et des composants des SII déployés à un PIS du gouvernement du Canada. [DSP 7.7.6.2] L'entrepreneur doit s'assurer que toutes les bases de données comprenant des données relatives au présent contrat et archivées ou entreposées sont isolées sur les plans physique et logique, en d'autres termes qu'elles n'ont aucune connexion directe ou indirecte de quelque type que ce soit avec d'autres bases de données.

SRTM 58	SC	5		PROTECTION CONTRE LES DÉNIS DE SERVICE	[EDT 2.6, paragraphe (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. [EDT 2.6, paragraphe (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. [EDT 2.6, paragraphe (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.
SRTM 59	SC	7		PROTECTION DES FRONTIÈRES	L'entrepreneur doit établir des zones de sécurité pour l'OEIE et le système de vérification des SII conformément aux lignes directrices du guide ITSG-22 du CSTC **[Section 3 Zones de sécurité de réseau dans le contexte de la sécurité des TI]**. [DSP 7.7.6.3] L'entrepreneur doit s'assurer qu'il est possible d'accéder aux données concernant ce contrat et de les traiter uniquement au Canada ou dans une administration autre approuvée par l'autorité contractante conformément au paragraphe (...).
SRTM 60	SC	7	(11)	PROTECTION DES FRONTIÈRES	[EDT 8.1, paragraphe (353.d)] L'entrepreneur doit limiter l'accès à l'OEIE par adresses IP et numéros de port d'application.
SRTM 61	SC	10		DÉCONNEXION RÉSEAU	L'entrepreneur doit s'assurer que les systèmes de frontière qui protègent l'OEIE mettent fin aux sessions de l'OEIE à la demande des utilisateurs finaux ou après 30 minutes d'inactivité.
SRTM 62	SC	12		ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES	[DSP 7.7.3.1] L'entrepreneur reconnaît que le Canada peut préciser qu'un équipement ou un réseau est sensible sur le plan de la sécurité et imposer une classification de sécurité auquel cas seuls les employés et les entrepreneurs ayant une cote de sécurité peuvent travailler au système. Les personnes qui ne possèdent pas cette habilitation peuvent seulement aider à travailler sur le système, mais ne sont pas autorisées à contrôler ou charger le logiciel.

					Le Centre de sûreté opérationnel (CSO) de l'entrepreneur doit comprendre un appareil terminal sécurisé (STE) fourni avec le matériel fourni par le gouvernement, selon les processus actuels du COMSEC, pour communiquer avec le Canada à la demande de ce dernier. Cet appareil doit comprendre un numéro de téléphone unique et spécifique. L'entrepreneur doit nommer un gardien COMSEC comme interface afin de faciliter la gestion de la clé cryptographique du STE et accomplir des tâches de mise à l'essai et de dépannage de base à la demande du Canada.
SRTM 63	SC	13		UTILISATION DE LA CRYPTOGRAPHIE	[EDT 3.6.6 (157)] 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 à des normes 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. [EDT 8.1, paragraphe (353.e)] L'entrepreneur doit mettre en œuvre le protocole TLS (Transport Layer Security) dans son OEIE [si une solution Web est mise en œuvre] et chiffrer les sessions à l'aide de l'algorithme 3DES (3 Key Triple Data Encryption Standard) ou AES (Advance Encryption Standard).
SRTM 64	SC	23	(1)	AUTHENTICITÉ DES SESSIONS	L'entrepreneur doit s'assurer que l'OEIE invalide les identificateurs de session lorsque l'utilisateur ferme sa session ou lorsque la session est terminée autrement.
SRTM 65	SC	23	(2)	AUTHENTICITÉ DES SESSIONS	L'OEIE doit prévoir une capacité de fermeture de session facilement observable.
SRTM 66	SI	2		CORRECTION DES DÉFAUTS	L'entrepreneur doit identifier et corriger les défauts de l'OEIE et du système de vérification des SII. L'entrepreneur doit intégrer la correction des défauts à son processus de gestion des configurations.

SRTM 67	SI	3	PROTECTION CONTRE LES CODES MALVEILLANTS	L'entrepreneur doit s'assurer que l'OEIE et les systèmes de vérification des SII sont protégés des conséquences directes et indirectes des codes malveillants.
SRTM 68	SI	4	SURVEILLANCE DES SYSTÈMES D'INFORMATION	a) L'entrepreneur doit surveiller les événements liés à l'OEIE, au système de vérification des SII et à l'infrastructure des SII pour détecter : i. les attaques contre le système d'information; ii. les conditions qui peuvent nuire à la disponibilité ou à l'intégrité des SII; iii. les preuves de manquement à l'obligation de confidentialité concernant les données protégées du Canada, y compris notamment le contenu des données enregistrées dans l'OEIE, le système de vérification des SII ou les systèmes de communication utilisés pour transmettre les données protégées ou les conversations vocales protégées. b) L'entrepreneur doit identifier et signaler au responsable technique de SPC les utilisations non autorisées du système et de l'infrastructure des SII, de l'OEIE et du système de vérification des SII. c) L'entrepreneur doit déployer des dispositifs de surveillance du matériel fourni par le gouvernement : i) stratégiquement dans ses installations et son infrastructure pour collecter l'information sur le service fourni au Canada qu'elle juge essentielle et ii) de manière aléatoire dans le système d'information pour faire le suivi des types de transaction qui l'intéressent particulièrement. d) L'entrepreneur doit fournir un mécanisme permettant l'acheminement de tout le trafic de couche IP surveillé à l'aide du matériel fourni par le gouvernement à un endroit de la région de la capitale nationale (RCN) précisé par le Canada. e) L'entrepreneur doit élever le niveau des activités de surveillance du système et de l'infrastructure des SII dès qu'il y a une indication de risque accru pour les activités et les biens de l'entrepreneur, les personnes, les autres organisations ou le Canada selon l'information relative à l'application de la loi, découlant du renseignement ou provenant d'autres sources crédibles. f) L'entrepreneur doit obtenir un avis juridique concernant les activités de surveillance du système d'information, conformément aux lois du gouvernement du Canada et aux politiques, directives et normes du SCT. [EDT 2.6, paragraphe (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 contre SPC pouvant éventuellement avoir des répercussions sur le réseau du

					gouvernement du Canada. Il doit également appliquer les mesures d'atténuation nécessaires, une fois qu'elles ont été approuvées par SPC.
SRTM 69	SI	4	(5)	SURVEILLANCE DES SYSTÈMES D'INFORMATION	[EDT 2.6, paragraphe (71)] L'entrepreneur doit fournir sur demande dans son infrastructure un service de nettoyage anti-déni de service distribué. [EDT 2.6, paragraphe (77)] L'entrepreneur doit transmettre au Canada des alertes presque en temps réel, par courriel ou message texte, selon les événements d'intrusion ou les éléments déclencheurs configurés. Les événements d'intrusion ou les éléments déclencheurs sont notamment : a) les canaux de contrôle des dénis de service à partir ou en provenance des points de déploiement des SII du Canada; b) les attaques de déni de service ou de déni de service distribué contre l'espace adresse du gouvernement du Canada.

SRTM 70	SI	5	ALERTES, AVIS ET DIRECTIVES DE SÉCURITÉ	a) L'entrepreneur doit recevoir régulièrement d'organisations externes désignées par le Canada des alertes, avis et directives de sécurité concernant le système d'information et y répondre. b) L'entrepreneur doit produire des alertes, avis et directives de sécurité internes lorsqu'il le juge nécessaire. c) L'entrepreneur doit diffuser des alertes, avis et directives de sécurité à tous les employés participant à l'administration, l'exploitation et l'examen du système, du service et de l'infrastructure des SII ou au traitement des incidents. d) L'entrepreneur doit mettre en œuvre les directives de sécurité transmises par le Canada sur les menaces élevées ou persistantes dans les délais prescrits. [DSP 7.7.2.2] L'entrepreneur reconnaît que le Canada a besoin des services de télécommunications fournis conformément au contrat, et il garantit qu'il les fournira toujours conformément au contrat. Il garantit aussi que ces services s'accompagneront de mesures de sécurité solides et exhaustives qui évolueront en même temps que les menaces de sécurité et les technologies, ce qui signifie que les mesures de sécurité utilisées doivent être mises à jour pendant toute la durée du contrat afin de réaliser le niveau le plus élevé possible d'intégrité, de disponibilité et de confidentialité des données. [DSP 7.7.2.3] L'entrepreneur doit mettre en œuvre toutes les mesures de sécurité ou de protection raisonnables demandées par le Canada de temps à autre, dans un délai raisonnable convenu avec le Canada. Les parties conviennent de déterminer le caractère raisonnable selon la gravité de la menace à l'intégrité, à la disponibilité et à la confidentialité des données et des communications du Canada. [EDT 2.6, paragraphe (91)] L'entrepreneur doit répondre aux demandes de SPC si ce dernier l'avise d'une cyber-menace imminente.
SRTM 71	SI	12	TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION	L'entrepreneur doit traiter et conserver l'information interne et celle produite par le service des SII conformément aux lois du gouvernement du Canada et aux politiques, directives et normes du SCT qui s'appliquent, ainsi qu'aux exigences opérationnelles.

SRTM 72	CA	7	SURVEILLANCE CONTINUE	[DSP 7.7.10.1] L'entrepreneur doit surveiller le réseau pour déceler les activités anormales ou douteuses, comme les heures de travail inhabituelles, les demandes non nécessaires de code ou de données, le mouvement anormal des données ou l'utilisation excessive des systèmes ou des ressources. [DSP 7.7.10.2] L'entrepreneur doit signaler immédiatement au responsable technique et à la DSIC tout incident relatif à la sécurité du réseau du Canada, de sa propre infrastructure ou de son réseau de base ou des données du Canada, si cela a une incidence sur le Canada, y compris les incidents décrits au paragraphe (7.6.12.1) [de la DSP]. Par exemple, tout accès ou toute tentative d'accès non autorisé doit être signalé immédiatement. Les virus, les programmes malveillants et l'installation non autorisée de code de logiciel doivent également être signalés sur-le-champ, peu importe leur emplacement.