Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

LIGNES DIRECTRICES SUR LA CHAÎNE D'APPROVISIONNEMENT DES TECHNOLOGIES (LDCAT)

CLAUSES CONTRACTUELLES LIÉES À L'ÉQUIPEMENT ET AUX SERVICES DE TÉLÉCOMMUNICATION

TSCG-01\G

Octobre 2010

Page intentionnellement laissée en blanc.

Avant-propos

Le document *Clauses contractuelles liées à l'équipement et aux services de télécommunication (TSCG-01|G)* est un document non classifié, publié avec l'autorisation du chef, Centre de la sécurité des télécommunications Canada (CSTC).

Les propositions de modification devraient être envoyées au représentant des Services à la clientèle de la Sécurité des technologies de l'information (TI) du CSTC par l'intermédiaire des responsables de la sécurité des TI du ministère.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC par courriel à itsclientservices@cse-cst.gc.ca ou par téléphone au 613-991-7654.

Date d'entrée en vigueur

La présente publication entre en vigueur le 15 octobre 2010.

Signé initialement par

_____

Colleen D'Iorio
Chef adjointe, intérimaire de la Sécurité des technologies de l'information

.

Table des matières

Liste des abréviations et acronymes

Acronyme	Description
ASI	Attestation de sécurité d'installation
CC	Critères communs
CSPC	Conseils en matière de sécurité pour les produits commerciaux
CSTC	Centre de la sécurité des télécommunications Canada
DP	Demande de proposition
DSIC	Direction de la sécurité industrielle canadienne
EMR	Évaluation des menaces et des risques
ESN	Exception au titre de la sécurité nationale
GC	Gouvernement du Canada
IPSec	Protocole IpSec
LVERS	Liste de vérification des exigences relatives à la sécurité
PVMC	Programmes de validation des modules cryptographiques
STI	Sécurité de la technologie de l'information
TCP	Transmission Control Protocol
TPSGC	Travaux publics et Services gouvernementaux Canada
UDP	User Datagram Protocol

Page intentionnellement laissée en blanc.

1 Introduction

En avril et mai 2008, de nombreuses réunions d'un groupe spécial des ministères du gouvernement fédéral ont eu lieu au sujet d'un problème de sécurité nationale émergent qui concernait la vulnérabilité de la chaîne d'approvisionnement de l'équipement et des services de télécommunication du gouvernement du Canada.

En plus d'être sensibilisé à la menace d'une cyberattaque, on prend de plus en plus connaissance des risques que posent des technologies potentiellement vulnérables ou modifiées qui peuvent pénétrer les réseaux de communications et l'infrastructure de technologie de l'information du gouvernement du Canada (GC) par l'intermédiaire de la chaîne d'approvisionnement.

Il est possible de réduire les risques en prévoyant des clauses de sécurité précises dans les contrats de TPSGC qui contribuent à assurer l'intégrité, la disponibilité et la confidentialité des données et des communications du pays.

Ces clauses ont été élaborées à partir d'un scénario de services de télécommunication gérés, où un entrepreneur assume la responsabilité de choisir, de mettre en œuvre, d'exploiter et d'assurer la maintenance d'une infrastructure et des services de télécommunications. Il a été déterminé qu'il n'est pas possible d'élaborer des clauses de sécurité idéales ou « universelles » en raison de l'évolution des menaces et de la variété et de la complexité des environnements opérationnels du GC et des besoins qui en découlent.

2 Portée

Les présentes lignes directrices décrivent un processus de sélection et d'adaptation des clauses contractuelles à intégrer dans les contrats de Travaux publics et Services gouvernementaux Canada (TPSGC) en vue de protéger l'intégrité, la disponibilité et la confidentialité des données et des communications du Canada dans le cadre d'approvisionnement de services gérés. L'objectif de l'application des clauses de sécurité dans ces contrats est de prévenir ou d'atténuer les risques associés à la chaîne d'approvisionnement. Certaines de ces clauses peuvent également servir à l'approvisionnement de solutions et d'équipement de télécommunication.

Les lignes directrices ne doivent pas être considérées comme une liste exhaustive de toutes les clauses possibles. Chaque exigence et les clauses contractuelles qui en découlent devraient être élaborées en gardant à l'esprit des menaces et des exigences en matière de sécurité précises. La sélection et l'adaptation des clauses devraient être faites en même temps qu'on remplit la Liste de vérification des exigences relatives à la sécurité (LVERS) pour les exigences relatives aux contrats et aux contrats de sous-traitance.

3 Compromis

Au moment de sélectionner et d'appliquer ces clauses dans les contrats d'approvisionnement, les utilisateurs devraient examiner attentivement l'incidence des mesures de sécurité retenues sur le coût, le calendrier et les exigences opérationnelles.

Les clients devraient chercher un compromis raisonnable entre le coût accru qu'imposent les exigences de sécurité et l'atténuation du risque qui découlerait du respect des exigences. Sur demande, TPSGC et le CSTC peuvent aider les clients dans ces décisions. Pour de plus amples renseignements sur les présentes lignes directrices, veuillez communiquer avec les services à la clientèle du CSTC.

4 Hypothèses

Il y a trois façons complémentaires de se pencher sur les problèmes de sécurité dans tout approvisionnement donné :

1. en incluant des exigences obligatoires ou cotées dans les critères d'évaluation qui rejettent à la présélection les technologies et les solutions de soumissionnaires non qualifiés. En ce qui concerne un approvisionnement régi par un accord commercial, il faut veiller à ce que les critères d'évaluation soient entièrement divulgués et conformes à l'accord commercial ou déterminer qu'une Exception au titre de la sécurité nationale (ESN) est appropriée et a été invoquée;
2. en imposant des engagements contractuels aux fournisseurs qui procurent une certaine assurance d'intégrité, de disponibilité et de confidentialité des réseaux et des données du Canada et atténuent les menaces et les vulnérabilités associées aux technologies potentiellement vulnérables ou modifiées;
3. en appliquant des mesures de sécurité du personnel, de sécurité physique et opérationnelle, par exemple, la Couronne peut exiger que les entrepreneurs soient accompagnés lorsqu'ils viennent sur les lieux.

Le présent document s'intéresse au point (2) – les clauses contractuelles qui peuvent être sélectionnées et adaptées aux contrats de Travaux publics et Services gouvernementaux Canada (TPSGC). Cependant, la prévention ou l'atténuation du risque pour la chaîne d'approvisionnement peut aussi être améliorée par les points (1) et (3).

5 Processus

Pour sélectionner et adapter les clauses contractuelles à intégrer dans les contrats de TPSGC, il faut suivre le processus décrit ci-dessous :

1. Les organismes de sécurité appropriés devraient offrir aux agents de négociation des contrats de TPSGC des séances d'information régulière sur la sécurité. Ces séances aideront à assurer que les agents de négociation des contrats de TPSGC sont au courant des menaces et des vulnérabilités courantes et des stratégies d'atténuation possibles;
2. sur réception d'une demande d'approvisionnement d'un ministère client pour un service, une solution ou une infrastructure importante de télécommunications ou de réseau géré :
    a. l'agent de négociation des contrats offre d'organiser, au besoin, une rencontre entre le CSTC ou un autre organisme de sécurité approprié et le ministère client afin de discuter des besoins, tout en faisant l'examen des exigences en matière de sécurité industrielles cernées dans la LVERS et les menaces connexes;
    b. le CSTC donne une rétroaction au client et à TPSGC sur les préoccupations relatives à la chaîne d'approvisionnement (ou autre) ou de sécurité (le cas échéant) associées à l'approvisionnement planifié;
    c. s'il est déterminé que des clauses de sécurité additionnelles sont requises pour atténuer les menaces, l'agent de négociation des contrats, de concert avec la DSIC et le CSTC, sélectionne et adapte les clauses de sécurité appropriées;
    d. l'agent de négociation des contrats finalise les clauses de sécurité et les soumet à un examen légal afin de déterminer si :
        i. elles sont raisonnablement nécessaires pour réaliser les objectifs de sécurité du Canada (et déterminer si certaines des clauses sont interreliées – p. ex. si une clause est supprimée, est-il important d'en conserver un autre);
        ii. elles sont conformes aux obligations commerciales du Canada (ce qui facilitera les décisions quant à savoir s'il est approprié d'invoquer l'ESN);
        iii. elles sont raisonnables d'un point de vue commercial (ce qui peut influencer la qualité et la quantité des soumissions);
        iv. elles sont conformes aux obligations de sécurité de la DSIC;
    e. cette évaluation légale fera l'objet de discussions entre le CSTC et le ministère client et une décision finale sera prise quant aux clauses, le cas échéant, à inclure dans le contrat.

6 Clauses de sécurité

Les clauses de sécurité décrites dans les pages suivantes sont précédées de la description de leur objectif.

Nota : On rappelle aux utilisateurs que les clauses devraient être modelées en fonction des besoins, des menaces et des vulnérabilités particuliers associés à l'exigence et à l'approvisionnement planifié.

6.1 Mesures de sécurité générales entourant la transmission de données sensibles

Objectif : La clause suivante vise à dissiper les inquiétudes concernant la transmission des données, particulièrement lorsqu'elles sont jugées sensibles.

(a) L'[équipement/service] de télécommunication fourni en vertu du contrat sera utilisé pour la transmission des données du gouvernement du Canada de divers genres, y compris les communications sécurisées (à divers niveaux de classification de sécurité), les communications privilégiées (comme les documents confidentiels du Cabinet et les communications assujetties au secret professionnel) et les communications autrement sensibles (y compris les transmissions contenant des renseignements personnels des Canadiens et des renseignements exclusifs ou confidentiels de tierces parties, comme les fournisseurs). [Nota à l'agent de négociation des contrats : si l'entrepreneur entend recueillir des renseignements personnels et les utiliser dans le cadre du travail, il faudrait songer à inclure les conditions générales supplémentaires 4008 (renseignements personnels) de TPSGC.]

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

(c) 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 que le caractère raisonnable sera déterminé en fonction de la gravité de la menace à l'intégrité, à la disponibilité et à la confidentialité des données et des communications du Canada.

6.2 Habilitation de sécurité

Objectif : La clause suivante vise à cerner les exigences d'habilitation de sécurité du personnel de l'entrepreneur qui a accès aux installations, à l'équipement ou aux données du système. Le niveau d'habilitation dépend du niveau de sensibilité de l'information et du caractère essentiel du système. Cette exigence devra se traduire dans la LVERS et dans le guide de sécurité qui l'accompagne pour l'approvisionnement.

Les niveaux de sécurité sont les suivants :

> **Confidentiel –** lorsqu'on peut raisonnablement s'attendre à ce que la compromission **cause un préjudice** à l'intérêt national.
>
> **Secret -** lorsqu'on peut raisonnablement s'attendre à ce que la compromission **cause un préjudice grave** à l'intérêt national.
>
> **Très secret -** lorsqu'on peut raisonnablement s'attendre à ce que la compromission **cause un préjudice exceptionnellement grave** à l'intérêt national.

En ce qui concerne l'article intitulé « Exigence de sécurité » :

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

(b) L'accès à distance à certains systèmes peut être permis (Confidentiel et Secret dans certains cas), mais toutes les frappes et le logiciel téléchargé doivent être copiés et gardés en preuve pour des fins judiciaires, le cas échéant.

(c) À l'arrivée dans les locaux du Canada, tout le personnel de l'entrepreneur et du sous-traitant (qui a été préapprouvé par l'autorité contractante), doit être en mesure de fournir une preuve d'emploi (comme une carte d'identification émise par l'entrepreneur ou le sous-traitant approuvé) et l'état d'habilitation de sécurité du personnel doit être déterminé par des sources sûres.

(d) Des personnes qui, même si elles n'ont pas accès à l'information ou des biens CLASSIFIÉS, peuvent occuper des postes qui sont jugés essentiels à l'intérêt national. Il s'agit entre autres du personnel qui a un accès privilégié offrant la possibilité de perturber ou d'endommager de façon importante des systèmes essentiels. Ces personnes doivent faire l'objet d'une enquête de sécurité et obtenir une habilitation de sécurité du niveau SECRET au moins. Par exemple, le personnel technique ou opérationnel, y compris les administrateurs ou les gestionnaires de réseau ou de système, qui contrôle directement les fonctionnalités les plus sensibles et indispensables comme la surveillance, la détection, la sauvegarde et la récupération de l'information, la mise à l'essai et l'installation de correctifs de sécurité, les changements de configuration au matériel et au logiciel de sécurité, la réaction aux incidents de sécurité, etc.

NOTA : les contrôles d'accès additionnels sont aussi requis comme la séparation des tâches afin d'assurer que personne n'a un accès trop grand aux fonctionnalités les plus sensibles. Des dossiers de vérification de sécurité doivent être disponibles afin d'assurer qu'un tel accès peut être suivi par vérification jusqu'à une personne en particulier.

(e) L'entrepreneur reconnaît que le Canada peut, en tout temps, refuser à une personne l'accès à ses locaux. Si l'individu satisfait les exigences d'habilitation de sécurité pour le type de travail qui est exécuté, mais que le Canada refuse de lui fournir l'accès nécessaire, en tout temps décrit dans le contrat pour achever la portion du travail qu'il doit exécuter, cette personne ne pourra pas débuter avant que le Canada n'ait informé l'entrepreneur que l'accès a été accordé à cette personne. Le Canada peut informer l'entrepreneur de sa raison pour refuser l'accès, mais peut aussi ne pas le faire s'il a déterminé, à sa discrétion, qu'il y avait des raisons de sécurité pour ne pas divulguer la raison.

(f) L'entrepreneur doit obtenir l'habilitation de sécurité requise pour tout son personnel avant l'attribution du contrat. Après l'attribution du contrat, il appartient uniquement à l'entrepreneur de s'assurer qu'il a un personnel complémentaire suffisant qui possède l'habilitation de sécurité nécessaire pour travailler au niveau requis dans le cadre du contrat.

(g) L'entrepreneur reconnaît que le Canada peut révoquer l'habilitation de sécurité d'une personne n'importe quand.

6.3 Sous-traitance

Objectif : La clause suivante vise à faire face aux situations où l'entrepreneur principal n'exécute pas tout le travail et qu'il faut approuver des sous-traitants afin de respecter la chaîne d'approvisionnement.

Sous-traitance :

(a) Malgré les conditions générales, aucune partie du travail ne peut se faire en sous-traitance (même par un affilié de l'entrepreneur) à moins d'avoir obtenu au préalable par écrit le consentement de l'autorité contractante. Pour obtenir le consentement de l'autorité contractante, l'entrepreneur doit fournir les renseignements suivants :

(i) le nom du sous-traitant;

(ii) la portion du travail à exécuter par le sous-traitant;

(iii) la vérification d'organisation désignée (VOD) ou le niveau d'Attestation de sécurité d'installation (ASI) du sous-traitant tel que requis par les travaux;

(iv) sur demande, l'état d'habilitation de sécurité des personnes employées par le sous-traitant qui devront accéder aux installations du Canada;

(v) la sous-LVERS signée par l'agent de sécurité de l'entreprise de l'entrepreneur à remplir par la DSIC;

(vi) tout autre renseignement requis par l'autorité contractante.

(b) Aux fins du présent article, n'est pas considéré un « sous-traitant » un fournisseur qui fait des affaires avec l'entrepreneur sans lien de dépendance avec lui et dont l'unique rôle est de fournir de l'équipement de télécommunications que l'entrepreneur utilisera pour assurer la prestation de services, notamment si l'équipement est installé dans le réseau de base ou l'infrastructure de l'entrepreneur.

6.4 Schéma de réseau

Objectif : La clause suivante s'applique aux services ou aux contrats de service gérés et aborde les situations où il y a une inquiétude quant à l'emplacement de l'équipement dans le réseau. L'entrepreneur serait tenu de fournir de l'information sur l'aménagement du réseau utilisé pour assurer les services.

Schéma de réseau :

(a) Dans les XX jours civils suivant l'attribution du contrat, l'entrepreneur est tenu de fournir à l'autorité technique une ébauche de schéma de réseau qui, à tout le moins, indique ce qui suit :

(i) la topologie de réseau physique et logique, dépeignant les nœuds et les connexions entre les nœuds dans le réseau;
(ii) les détails des nœuds dans le réseau, des protocoles, des largeurs de bande, etc.

(b) L'entrepreneur est tenu de fournir un schéma de réseau à jour au Canada à la fin de la période de mise en œuvre (le cas échéant) et par la suite [à tous les semaines/mois/trimestres], dans les deux semaines suivant la fin de chaque période de rapport, qui doit refléter tous les changements apportés au réseau au cours de la période du rapport. Même lorsqu'il n'y a pas de modifications, l'entrepreneur est tenu de refaire le schéma de réseau avec de nouvelles dates à tout le moins [à tous les semaines/mois/trimestres].

(c) L'entrepreneur reconnaît que le schéma de réseau ne lui est pas exclusif.

6.5 Assurance du produit et équipement et inventaire

Objectif : La clause suivante vise à procurer au Canada une liste complète de l'équipement utilisé pour la prestation des services de réseau. L'approche devrait être que, lorsque c'est possible, seuls les produits certifiés selon les critères communs (CC) et validés selon le Programmes de validation des modules cryptographiques (PVMC) sont sécurisés. Les exigences de certification devraient être énumérées dans les critères d'évaluation obligatoires ou dans la spécification. Il faudrait noter que les exigences de certification/validation peuvent avoir une incidence sur les objectifs liés aux coûts et au temps de l'approvisionnement planifié.

Équipement et inventaire :

(a) Dans les XX jours civils suivant l'attribution du contrat, l'entrepreneur doit présenter à l'autorité technique un inventaire complet de l'équipement déployé dans le réseau du Canada qui, à tout le moins, porte sur ce qui suit :

(i) l'équipement appartenant à l'entrepreneur;
(ii) l'équipement appartenant au Canada;
(iii) l'équipement appartenant à une tierce partie (qui identifie la tierce partie);
(iv) le fabricant de l'équipement et le pays d'origine;
(v) le modèle et le numéro de série de l'équipement;
(vi) l'endroit où chaque pièce d'équipement est installée (référence à l'exigence du schéma de réseau décrit à la section 6.4 précédente);
(vii) la date à laquelle l'équipement est installé;
(viii) la date à laquelle l'équipement a été entretenu pour la dernière fois (s'il s'agissait d'un entretien préventif ou correctif);

(ix) la date à laquelle le micrologiciel a été mis à jour la dernière fois.

(b) L'inventaire d'équipement doit être intégré aux schémas de réseau requis à la section 6.4 précédente de sorte qu'en révisant l'inventaire, le Canada peut immédiatement trouver le schéma de réseau où une pièce d'équipement individuelle a été déployée au sein du réseau (et inversement).

(c) L'entrepreneur doit fournir un inventaire d'équipement à jour au Canada à la fin de la période de mise en œuvre (le cas échéant) et par la suite [à tous les semaines/mois/trimestres], dans les deux semaines à la fin de chaque période de rapport, qui doit refléter tous les changements apportés au réseau au cours de la période du rapport.

(d) L'entrepreneur reconnaît que l'inventaire d'équipement ne lui est pas exclusif.

(e) Avant de mettre en œuvre les services de réseau, l'entrepreneur doit fournir à l'autorité technique une liste complète des :

(i) fabricants (et tout revendeur, si l'entrepreneur n'achète pas l'équipement directement du fabricant) de tout l'équipement qu'il déploiera dans le réseau du Canada dans le cadre des travaux;
(ii) fabricants (et tout revendeur, si l'entrepreneur n'achète pas l'équipement directement du fabricant) de tout l'équipement qu'il a déployé ou qu'il déploiera dans son infrastructure de réseau qui lui appartient ou celui d'une tierce partie ou son infrastructure de base qui sera interconnectée au réseau du Canada dans le cadre des travaux.

(f) À tout moment au cours du contrat, si l'entrepreneur propose de commencer le déploiement de l'équipement d'un nouveau fabricant dans le réseau du Canada ou sur la propre infrastructure de l'entrepreneur ou celle d'une tierce partie qui sera interconnectée au réseau du Canada, il doit tout d'abord obtenir l'approbation écrite de l'autorité technique.

(g) L'entrepreneur ne doit pas déployer d'équipement sur le réseau du Canada ou sur sa propre infrastructure ou celle d'une tierce partie ou sur son réseau de base ou sur celui d'une tierce partie qui sera interconnecté au réseau du Canada, à moins que l'équipement ait été évalué à l'externe par un organisme de certification reconnu, approuvé par le Canada. (Nota : une liste des organismes de certification qui sont reconnus au moment de l'attribution du contrat ou de la Demande de proposition (DP) devrait accompagner la DP et subséquemment être ajoutée au contrat.)

(h) À tout moment au cours du contrat, si le Canada avise l'entrepreneur qu'un fabricant donné n'est plus considéré fiable, l'entrepreneur (et ses sous-traitants) doit immédiatement cesser de déployer cet équipement dans le réseau du Canada et dans toute l'infrastructure ou le réseau de base de l'entrepreneur qui s'interconnectera au réseau du Canada. En ce qui concerne l'équipement déjà déployé, l'entrepreneur doit identifier et/ou enlever l'équipement de ce fabricant dans le réseau et dans toute l'infrastructure ou le réseau de base de l'entrepreneur qui s'interconnectera au réseau du Canada.

(i) Si l'entrepreneur est conscient qu'une tierce partie (autre que le sous-traitant) déploie de l'équipement non sécurisé sur son réseau, il doit immédiatement en aviser l'autorité technique.

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

Objectif : La clause suivante vise à assurer que le Canada a le contrôle sur l'emplacement des bases de données, du trafic et des données de réseau, lorsqu'il y a des préoccupations quant à certaines administrations ou à certaines de leurs lois.

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

(a) L'entrepreneur doit s'assurer que toutes les bases de données contenant l'information relative aux travaux (y compris les renseignements sur la facturation et/ou les détails d'appel) ou les données se trouvent au Canada ou, si l'autorité contractante a d'abord consenti par écrit, à une administration autre où :

(i) les protections équivalentes sont accordées aux renseignements personnels comme au Canada en vertu d'une loi comme la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* et en vertu de toute politique applicable du gouvernement du Canada;

(ii) les lois ne permettent pas au gouvernement de cette administration ou toute autre entité ou personne de chercher à obtenir ou d'obtenir le droit d'afficher ou de copier de l'information relativement au présent contrat sans obtenir tout d'abord le consentement écrit de l'autorité contractante.

(b) En ce qui concerne l'accord de son consentement à localiser une base de données dans une administration autre que le Canada, l'autorité contractante peut exiger de l'entrepreneur qu'il fournisse un avis légal d'un avocat qualifié dans une administration

étrangère indiquant que les lois dans cette administration satisfont les exigences décrites précédemment, ou peut exiger que l'entrepreneur paie pour que le Canada obtienne un tel avis légal. Le Canada a le droit de refuser toute demande d'héberger ses données dans une administration autre la sienne s'il y a un fondement raisonnable d'être préoccupé au sujet de la confidentialité, de la disponibilité ou de l'intégrité des données du Canada. Le Canada peut aussi exiger que toute donnée envoyée ou traitée à l'extérieur du pays soit chiffrée avec une cryptographie approuvée par le Canada et que la clé privée requise pour déchiffrer les données soit conservée au Canada conformément aux processus de gestion et de stockage des clés approuvés par le Canada.

(c) L'entrepreneur doit assurer que toutes les bases de données dans lesquelles les données relatives à ce contrat sont stockées/archivées sont indépendantes d'un point de vue physique et logique (ce qui signifie qu'il n'y a pas de lien direct ou indirect de quelque nature) de toutes les autres bases de données, à moins que ces bases de données se trouvent au Canada (ou dans une administration autre approuvée par l'autorité contractante en vertu de l'alinéa (a) et autrement satisfont les exigences du présent article).

(d) L'entrepreneur doit s'assurer qu'il est possible d'accéder aux données relatives à ce contrat et de les traiter uniquement au Canada ou dans une administration autre approuvée par l'autorité contractante en vertu de l'alinéa (a).

(e) L'entrepreneur doit s'assurer que tout le trafic de réseau national (c'est-à-dire le trafic émanant d'une partie du Canada à une destination ou une personne qui se trouve dans une autre partie du Canada) est acheminé exclusivement par le Canada, à moins que l'autorité contractante ait d'abord consenti par écrit à une voie de rechange. L'autorité contractante examinera les demandes pour acheminer le trafic intérieur par la voie d'une autre administration qui satisfait les exigences de l'alinéa (a).

6.7 Connectivité et contrôle d'accès au réseau

Objectif : La clause suivante vise à gérer l'accès autorisé par opposition à celui qui n'est pas autorisé aux réseaux et aux bases des données du Canada.

Connectivité et accès au réseau :

(a) L'entrepreneur doit protéger le réseau et toutes les bases de données y compris les données ou l'information du Canada à son sujet en tout temps en prenant toutes les mesures raisonnablement nécessaires pour sécuriser et protéger son intégrité et sa confidentialité. À cette fin, à tout le moins, l'entrepreneur doit :

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

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

(iii) protéger tous les systèmes informatiques ou les bases de données où sont stockées les données du Canada contre un accès externe à l'aide des méthodes habituellement utilisées, de temps à autre, par les organismes du secteur public et privé prudents au Canada dans le but de protéger les renseignements hautement protégés ou sensibles.

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

(c) À moins que l'autorité technique n'en fasse la demande, l'entrepreneur doit désactiver tous les ports d'écoute TCP/UDP de tout équipement déployé dans un réseau du Canada ou l'infrastructure ou le réseau de base de l'entrepreneur auquel le réseau du Canada est connecté. Des méthodes de contrôle d'accès strictes doivent être en place pour tous les ports ouverts aux fins de gestion du réseau.

(d) L'entrepreneur doit maintenir un journal de vérifications qui enregistre automatiquement toutes les tentatives d'accès au réseau du Canada, ainsi qu'à toutes les bases de données qui contiennent des données ou de l'information du Canada tenues à jour par l'entrepreneur au sujet du Canada (comme les renseignements sur la facturation et les renseignements sur les détails d'appel). Chaque action, transaction ou fonction opérationnelle exécutée sur le réseau, les systèmes ou les bases de données de l'entrepreneur liée au contrat doit pouvoir être retracée jusqu'à un utilisateur ou un compte individuel (en s'assurant que les identificateurs et les comptes d'utilisateur sont uniques et ne peuvent pas être partagés ou transférés d'une personne à une autre).

6.8 Protocoles de gestion de réseau

Objectif : La clause suivante aborde la gestion des réseaux du Canada. En collaboration avec le CSTC, il pourrait être approprié d'établir un plus grand nombre de recommandations ou d'exigences de sécurité de base techniques pour l'accès à distance. La clause ne porte pas sur des mesures de protection, des approches ou des techniques précises qui pourraient devenir obsolètes

au cours de la durée du contrat. Étant donné que la technologie du réseau évolue rapidement, il est recommandé que les ministères clients communiquent avec le CSTC afin de mettre à jour les questions de sécurité ou les menaces à l'appui de la planification des exigences et de l'approvisionnement.

Protocoles de gestion de réseau :

(a) L'entrepreneur doit s'assurer que [l'équipement/tous les composants qui font partie du système utilisé pour assurer la prestation des services de réseau] peut être géré à l'aide de protocoles sécurisés.

(b) Si l'entrepreneur utilise des serveurs de gestion qui ont un niveau de sécurité ou de chiffrement configurable, l'entrepreneur doit désactiver tous les niveaux autres que le niveau le plus élevé de sécurité et/ou de chiffrement.

(c) L'entrepreneur ne doit pas utiliser de protocoles qui transmettent par le réseau des noms d'utilisateur ou des mots de passe en texte clair le réseau.

(d) L'entrepreneur ne doit pas utiliser les protocoles (et doit les désactiver) qui ne peuvent pas passer par des coupe-feu compatibles avec la session.

(e) Le Canada ne considérera pas qu'un protocole autrement non sécurisé est sécurisé même s'il a fait l'objet de l'utilisation de techniques de tunnelisation comme la redirection de port ou le protocole IpSec (IPSec).

(f) 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.

6.9 Évaluation et gestion de la vulnérabilité

Objectif : La clause suivante traite de la vulnérabilité de l'équipement déployé dans le réseau.

Évaluation et gestion de la vulnérabilité :

(a) L'entrepreneur doit fournir à l'autorité technique de l'information opportune au sujet des vulnérabilités (c.-à-d. toutes les faiblesses ou les lacunes de conception cernées dans [tout équipement fourni en vertu du contrat/composant qui fait partie du système utilisé pour assurer la prestation des services de réseau) qui permettrait à une personne non autorisée de compromettre l'intégrité, la confidentialité, les contrôles d'accès, la disponibilité, l'uniformité ou le mécanisme de vérification du système ou des données et des applications qu'il héberge.

(b) Lorsqu'une vulnérabilité est causée par l'équipement ou le code de logiciel fabriqué ou écrit par l'entrepreneur ou l'un de ses sous-traitants, l'entrepreneur doit immédiatement corriger la vulnérabilité à ses propres frais.

(c) Lorsqu'une vulnérabilité est causée par l'équipement ou le code de logiciel fabriqué ou écrit par une tierce partie (autre qu'un sous-traitant), en plus d'aviser l'autorité technique de la vulnérabilité dès qu'il est mis au courant, l'entrepreneur doit mettre en œuvre les mises à niveau, les correctifs ou toute autre mesure corrective dans un délai acceptable pour le Canada une fois qu'ils ont été mis à la disposition par le fabricant ou l'éditeur de logiciel, aux propres frais de l'entrepreneur, à moins que l'autorité technique ne fasse abstraction de cette exigence (en regard d'une mise à niveau, d'un programme ou mesure de correction) par écrit.

6.10 Résilience de la chaîne d'approvisionnement et du plan de reprise après sinistre

Objectif : La clause suivante vise à gérer la continuité des activités et la reprise après sinistre.

Résilience de la chaîne d'approvisionnement et du plan de reprise après sinistre :

(a) Dans les XX jours civils suivant l'attribution du contrat, l'entrepreneur doit présenter à l'autorité technique l'ébauche d'un plan de continuité des activités qui, à tout le moins, porte sur ce qui suit :

(i) les mesures que l'entrepreneur prendra si l'un de ses principaux fournisseurs se retire des affaires;
(ii) les mesures que l'entrepreneur prendra si l'un de ses principaux fournisseurs est identifié comme un qui ne fournit plus d'équipement « fiable »;
(iii) les mesures que l'entrepreneur prendra si une partie du réseau est endommagée par une cause « naturelle » (force majeure) ou un acte malveillant.

Le paragraphe suivant décrit les options du Canada si le fournisseur ne peut pas garantir la disponibilité du service en raison d'un cyberévénement ou d'une cyberattaque contre l'infrastructure du fournisseur.

(b) L'entrepreneur doit dissiper les préoccupations soulevées par le Canada au sujet de l'ébauche du plan avant de finaliser le plan de continuité des activités. Dans les 30 jours civils de chaque date anniversaire du contrat, l'entrepreneur doit fournir à l'autorité technique une mise à jour de son plan de continuité des activités.

(c) Dans les XX jours civils suivant l'attribution du contrat, l'entrepreneur doit fournir à l'autorité technique une ébauche de plan de reprise après sinistre qui, à tout le moins, porte sur ce qui suit :

(i) la fréquence (pas moins de XX fois) à laquelle les sauvegardes de secours des bases de données et des systèmes seront faites;
(ii) la fréquence (pas moins de XX fois) à laquelle le plan de reprise après sinistre de l'entrepreneur sera mis à l'essai.

L'entrepreneur doit aborder les préoccupations soulevées par le Canada au sujet de l'ébauche du plan avant de finaliser le plan de reprise après sinistre. Dans les 30 jours civils suivant chaque date anniversaire du contrat, l'entrepreneur doit fournir à l'autorité technique une mise à jour de son plan de reprise après sinistre.

(d) Les dispositions pour la mise en main tierce du code source [pour une discussion fondée sur les besoins et les menaces].

6.11 Sécurité physique

Objectif : La clause suivante porte sur les exigences de sécurité physique applicables aux locaux de l'entrepreneur dans l'utilisation des contrats de service.

Sécurité physique :

(a) L'entrepreneur doit fournir un niveau [sélectionner le niveau] de sécurité physique pour [dresser la liste des composants du réseau].

6.12 Évaluation des menaces et des risques

Objectif : La clause suivante concerne les menaces et les risques qui pourraient compromettre les réseaux ou les services canadiens assurés par l'entrepreneur. Cette clause s'ajouterait à l'évaluation des menaces et des risques (EMR) requise pour l'accréditation d'un système.

Nota : On pourrait songer à exiger que le soumissionnaire se conforme à la norme ISO 27001/29100 ou fournisse les produits livrables comme « une évaluation des risques de la chaîne d'approvisionnement », mais le coût et la valeur de telles mesures devraient être examinés attentivement si les organismes de sécurité reconnaissent que le soumissionnaire est affilié à des technologies qui ne sont pas jugées fiables.

Évaluation des menaces et des risques :

Dans les XX jours civils suivant l'attribution du contrat, l'entrepreneur doit présenter à l'autorité contractante et à la DSIC une évaluation des menaces et des risques qui doit inclure :

(a) une liste de tout le personnel à qui l'entrepreneur a accordé l'accès au réseau ou aux données du Canada et le niveau d'habilitation de sécurité accordé à chaque personne par la DSIC;

(b) une description de toutes les mesures prises par l'entrepreneur (et, le cas échéant, ses sous-traitants) pour protéger l'infrastructure du réseau et le réseau de base;

(c) une description de toutes les mesures prises par l'entrepreneur (et, le cas échéant, ses sous-traitants) pour protéger le réseau du Canada;

(d) une description de toutes les mesures prises par l'entrepreneur (et, le cas échéant, ses sous-traitants) pour protéger les données du Canada;

(e) une explication détaillée des menaces potentielles ou réelles au réseau ou aux données du Canada [supprimer s'il n'y a pas d'accès aux données du Canada], ainsi qu'une évaluation des risques découlant de ces menaces et la pertinence des mesures de protection en place pour prévenir ces risques;

(f) une explication de toute nouvelle mesure que l'entrepreneur entend mettre en œuvre pour protéger le réseau et les données du Canada;

(g) tout renseignement raisonnable demandé par l'autorité technique de temps en temps, y compris les renseignements requis par l'autorité technique, pour effectuer sa propre évaluation des menaces et des risques conformément aux politiques applicables du gouvernement du Canada.

Dans les 30 jours civils de chaque date anniversaire du contrat et en tout temps si l'autorité technique le demande, l'entrepreneur doit fournir à l'autorité technique une mise à jour de son évaluation des menaces et des risques.

6.13 Surveillance de sécurité et rapport d'incident

Objectif : La clause suivante aborde l'utilisation anormale et non autorisée du réseau.

Surveillance de sécurité et signalement d'incident :

(a) L'entrepreneur doit surveiller les activités anormales ou suspectes dans le réseau comme les heures de travail inusitées, des demandes de code ou de données inutiles, des mouvements de données anormales ou une utilisation excessive des systèmes ou des ressources.

(b) L'entrepreneur doit signaler immédiatement à l'autorité technique et à la DSIC tout incident relatif à la sécurité du réseau canadien ou à son infrastructure ou au réseau de base de l'entrepreneur ou aux données du Canada, s'il y a une incidence sur le Canada, y compris entre autres les incidents décrits dans (a). Par exemple, tout accès non autorisé ou tentative d'obtenir un accès non autorisé doit immédiatement être signalé. Aussi, la découverte de tout virus ou code malveillant ou de l'installation d'un code de logiciel non autorisé sur l'équipement doit immédiatement être signalée.

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

6.14 Vérification de sécurité

Objectif : La clause suivante vise à permettre au Canada de vérifier la conformité de l'entrepreneur aux exigences de sécurité dans les contrats de service.

Vérification de sécurité :

Le Canada peut vérifier en tout temps la conformité de l'entrepreneur aux exigences de sécurité incluses dans le contrat. Si l'autorité contractante en fait la demande, l'entrepreneur doit fournir au Canada (ou à un représentant autorisé) en tout temps jugé raisonnable le plein accès à ses locaux, ses réseaux et à toutes les bases de données qui conservent des données du Canada ou des données relatives au contrat. Si le Canada cerne des lacunes de sécurité au cours d'une vérification, l'entrepreneur doit immédiatement les corriger à ses propres frais.

6.15 Changement de contrôle

Objectif : La clause suivante vise à exiger de l'entrepreneur d'obtenir l'approbation du Canada et de la DSIC pour un changement de contrôle. Aux fins des conditions générales, le terme « affectation » inclut entre autre un changement dans le contrôle si l'entrepreneur est constitué en société, qu'il s'agisse d'un changement direct ou indirect dans le contrôle réel de cette société, découlant de la vente, d'engagements ou d'autres dispositions des parts ou de tout autre moyen. Actuellement, les conditions normales de TPSGC exigent le consentement d'une affectation (qui est requise si l'entrepreneur vend ses biens à une autre société qui propose de prendre la relève

dans l'exécution du contrat), mais aucun consentement n'est requis si une autre société entend acheter toutes les parts requises pour changer de contrôle. D'une perspective de la sécurité, il est attendu pour certains contrats que le consentement du Canada sera requis pour un changement de contrôle.

Dans le cas d'un changement de contrôle, l'entrepreneur doit aviser l'autorité contractante immédiatement. Si le Canada détermine que le changement de contrôle pose un risque de sécurité au Canada, il se réserve le droit de résilier le contrat à sa guise.

7 Conclusion

L'objectif d'appliquer ces clauses dans les contrats est de prévenir ou d'atténuer les risques associés à la chaîne d'approvisionnement d'équipement et de services de télécommunication du gouvernement du Canada. Le présent document sera mis à jour périodiquement selon les leçons apprises.