Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0A1 / Noyau 0A1
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet
PAD-PRE-AUTHORIZED DEBIT RECEIPTS

Solicitation No. - N° de l'invitation	Date
EN891-130776/A	2012-11-13

Client Reference No. - N° de référence du client
20130776

GETS Reference No. - N° de référence de SEAG
PW-$$ZG-410-25088

File No. - N° de dossier	CCC No./N° CCC - FMS No./N° VME
410zg.EN891-130776	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2012-12-18

Time Zone
Fuseau horaire
Eastern Standard Time
EST

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Gagnon, Jocelyne C.	410zg

Telephone No. - N° de téléphone	FAX No. - N° de FAX
(819) 956-0575 ( )	(819) 956-2675

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA
PORTAGE III
11 LAURIER ST
Gatineau
Quebec
K1A0S5
Canada

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée	Delivery Offered - Livraison proposée
See Herein	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Business Management and Consulting Services Division / Division des services de gestion des affaires et de consultation
11 Laurier St. / 11, rue Laurier
10C1, Place du Portage
Gatineau, Québec K1A 0S5

Canada

TABLE DES MATIÈRES

PARTIE 7 - CLAUSES DU CONTRAT SUBSÉQUENT

1. Énoncé des travaux
2. Clauses et conditions uniformisées
3. Exigences relatives à la sécurité
4. Durée du contrat
5. Responsables
6. Paiement
7. Instructions relatives à la facturation
8. Attestations
9. Lois applicables
10. Ordre de priorité des documents
11. Ressortissants étrangers (entrepreneur canadien) et/ou Ressortissants étrangers (entrepreneur étranger)
12. Assurance

Liste des annexes :

Annexe A Énoncé des travaux

Annexe B Base de paiement

Annexe C Liste de vérification des exigences relatives à la sécurité

- Pièce jointe 1 de l’annexe C, Exigences en matière de Sécurité de la Technologie de l’information (TI)

PARTIE 1 - RENSEIGNEMENTS GÉNÉRAUX

1. Introduction

La demande de soumissions contient sept (7) parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

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

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires les instructions pour préparer leur soumission;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, s'il y a lieu, ainsi que la méthode de sélection;

Partie 5 Attestations : comprend les attestations à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences: comprend des exigences particulières auxquelles les soumissionnaires doivent répondre; et

Partie 7 Clauses du contrat subséquent: contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent**.**

Les pièces jointes comprennent le Barème de prix, les Critères techniques, les Attestations pour le Code de conduite - Attestations préalables à l'attribution du contrat et les Attestations additionels préalables à l'attribution du contrat.

Les annexes comprennent l'Énoncé des travaux*,* la Base de paiement, la Liste de vérification des exigences relatives à la sécurité

2. Sommaire

2.1 L'objectif premier est de fournir un seul fournisseur de services, ci-après dénommé entrepreneur, afin de traiter tous les débits pré-autorisés (DPA) en dollars canadiens au nom du Canada.
Un DPA est une opération initiée par un ministère ou un organisme gouvernemental pour commencer des déductions pré-autorisées d'un montant fixe ou variable, sur une base récurrente ou sporadique, directement sur le compte bancaire du payeur. Les DPAs sont autorisés par des accords écrits ou électroniques entre le payeur et le ministère ou l'organisme responsable.

2.2 Les services doivent être livrés au niveau national et sont requis à compter de la date d'attribution du contrat jusqu'au 31 mars 2016, avec une option irrévocable de la part du Canada d'étendre la durée du contrat d'un maximum de deux périodes supplémentaire d'un (1) an et une période additionelle de quatre (4) mois selon les mêmes conditions afin d'assurer un transition si nécessaire.

2.3 Ce besoin comporte des exigences relatives à la sécurité. Veuillez consulter :

- L'article 1, Exigences relatives à la sécurité, de la partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences.

- L’article 3, Exigences relatives à la sécurité, de la partie 7, Clauses du contrat subséquent.
- L’Annexe C, Liste de vérification des exigences relatives à la sécurité, et les pièces-jointes connexes.

Les soumissionnaires qui ne répondent pas, à l'heure actuelle, aux exigences en matière d'attestation de sécurité d'installation ou dont le personnel ne satisfait pas aux exigences doivent lancer le processus immédiatement en vue d'obtenir une attestation de sécurité, en demandant le parrainage de l'autorité contractante. Pour toute demande de renseignements sur les exigences en matière de sécurité, les soumissionnaires doivent communiquer avec la DSIC, au 1-866-368-4646 ou au 613-948-4176, dans la région de la capitale nationale. Ils peuvent également consulter le site Web de la DSIC à l'adresse suivante : http://ssi-iss.tpsgc-pwgsc.gc.ca/index-fra.html.

3. Compte rendu

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

PARTIE 2 - INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

1. Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le *Guide des clauses et conditions uniformisées d'achat* (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003, (2012-11-09) Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

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

Les soumissionnaires doivent fournir, avec leur soumission ou le plus tôt possible après le dépôt de celle-ci, une liste complète de tous les individus qui sont actuellement administrateurs du soumissionnaire. Si la liste n'a pas été fournie à la fin de l'évaluation des soumissions, le Canada informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Le défaut de fournir cette liste dans les délais prévus aura pour conséquence que la soumission sera déclarée non recevable. Les soumissionnaires doivent toujours fournir la liste des administrateurs avant l'attribution du contrat.

Le Canada peut, à tout moment, demander au soumissionnaire de fournir un formulaire de consentement dûment rempli et signé (Consentement à la vérification de l'existence d'un casier judiciaire - PWGSC-TPSGC 229) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/formulaires-forms-fra.html) pour toute personne inscrite sur la liste susmentionnée, et ce dans un délai précis. Le défaut de fournir le formulaire de consentement dans les délais prévus aura pour conséquence que la soumission sera déclarée non recevable.

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

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

Le paragraphe 5.4 du document 2003, Instructions uniformisées - biens ou services - besoins concurrentiels, est modifié comme suit :

Supprimer : soixante (60) jours
Insérer : cent-vingts (120) jours civils.

1.1 Clauses du Guide des CCUA

A7035T (2007-05-25), Liste des sous-traitants proposés

2. Présentation des soumissions

Les soumissions doivent être présentées uniquement au Module de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions. Les soumissions transmises à TPSGC par courrier électronique ne seront pas acceptées.

En raison du caractère de la demande de soumissions, les soumissions transmises par télécopieur à l'intention de TPSGC ne seront pas acceptées.

3. Demandes de renseignements - en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins dix (10) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions, ou demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les soumissionnaires.

4. Lois applicables

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

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

5. Fondement du titre du Canada sur les droits de propriété intellectuelle

Le ministère des Travaux Publics et Services Gouvernementaux Canada a déterminé que tout droit de propriété intellectuelle découlant de l'exécution des travaux prévus par le contrat subséquent appartiendra au Canada, pour les motifs suivants :

lorsque le matériel créé ou conçu se compose de matériel protégé par le droit d'auteur, sauf dans le cas des logiciels informatiques et de la documentation s'y rapportant.

PARTIE 3 - INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

1. Instructions pour la préparation des soumissions

Le Canada demande que les soumissionnaires fournissent leur soumission en sections distinctes, comme suit:

Section I : Soumission technique (4 copies papier*)*;
Section II : Soumission financière (1 copie papier*)*; et
Section III: Attestations (1copies papier*)*.

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

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

(a) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm); et
(b) utiliser un système de numérotation correspondant à celui de la demande de soumissions.

En avril 2006, le Canada a approuvé une politique exigeant que les agences et ministères fédéraux prennent les mesures nécessaires pour incorporer les facteurs environnementaux dans le processus d'approvisionnement Politique d'achats écologiques (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html).

Pour aider le Canada à atteindre ses objectifs, on encourage les soumissionnaires à:

1) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et/ou contenant au moins 30 % de matières recyclées; et

2) utiliser un format qui respecte l'environnement: impression noir et blanc, recto-verso/à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ni reliure à anneaux.

Section I : soumission technique

Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires devraient démontrer leur capacité et décrire l'approche qu'ils prendront de façon complète, concise et claire pour effectuer les travaux.

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indicant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

Section II : soumission financière

1.1 Les soumissionnaires doivent présenter leur soumission financière en dollars canadiens et en conformité avec le barème de prix détaillé dans la pièce jointe 1 de la Partie 3. Le montant total de la taxe

sur les produits et services (TPS) ou de la taxe de vente harmonisée (TVH) doit être indiqué séparément, s'il y a lieu.

1.2 Les soumissionnaires doivent soumettre leur prix FAB destination; les droits de douane et les taxes d'accise canadiens compris, s'il y a lieu; et la TPS ou la TVH exclue.

1.3 Au moment de préparer leur soumission financière, les soumissionnaires devraient examiner la base de paiement à l'annexe "B" et la clause 1.2, Évaluation financière, figurant à la Partie 4.

1.4 Les soumissionnaires devraient inclure l'information suivante dans leur soumission financière:

1. leur appellation légale;
2. leur numéro d'entreprise - approvisionnement (NEA); et
3. Le nom de la personne-ressource (y compris son adresse postale, ses numéros de téléphone et télécopieur, et son adresse courriel) autorisée par le soumissionnaire à entrer en communications avec le Canada relativement:
   a. à leur soumission; et
   b. à tout contrat subséquent pouvant découler de leur soumission.

1.5 Clauses du Guide des CCUA

C3011T (2010-01-11), Fluctuation du taux de change

Section III: Attestations

Les soumissionnaires devraient inclure dans la Section III les attestations exigées à la Partie 5.

PIÈCE JOINTE 1 DE LA PARTIE 3
BARÈME DE PRIX

Le soumissionnaire devrait remplir ce barème de prix et le joindre ensuite à sa soumission financière. Au minimum, le soumissionnaire doit répondre à ce barème de prix dans sa soumission financière en y incluant, pour chacune des périodes précisées ci-dessous, le prix ferme tout compris (en dollars canadiens) proposé pour chacune des catégories ciblées.

En incluant des données volumétriques dans le présent document, le Canada ne garantit pas pour autant que son utilisation future des services décrits aux présentes correspondra à ces données.

Voici les seules catégories de frais qui peuvent être proposées :

A. Frais de transaction de débit préautorisé (DPA)
B. Frais de transaction d'effets retournés

REMARQUE : Tous les autres coûts facturés au soumissionnaire doivent être recouvrés à partir des frais susmentionnés.

1.0 Calcul du prix total évalué

Aux fins d'évaluation uniquement, le prix total évalué correspondra à la somme des éléments A et B décrits ci-dessous.

A. Frais de transaction de DPA :

Il s'agit des frais de transaction fermes tout compris de chaque débit figurant dans le fichier de DPA transmis par le receveur général, lequel fichier passe l'étape initiale de validation de l'entrepreneur et est finalement joint aux fichiers de DPA transmis aux institutions financières afin d'effectuer le débit à partir des comptes des clients. Les frais de transaction tout compris doivent tenir compte de toutes les exigences relatives au traitement et à l'établissement de rapports.

Directives

a) Les soumissionnaires devraient établir clairement les frais fermes tout compris de chaque fourchette annuelle des volumes et de chaque année dans les tableaux A1 et A2 (colonnes B, D, F, I et K).
b) Si un soumissionnaire souhaite offrir des frais fixes, peu importe le volume, il doit indiquer des frais identiques dans chaque fourchette des volumes dans les tableaux A1 et A2.
c) Les frais annuels fermes tout compris des transactions de DPA seront calculés de la manière suivante : (somme des coefficients de pondération des prix de la fourchette des volumes) × (volumes annuels prévus de DPA). Ce calcul sera effectué dans les tableaux A1 et A2.
d) Les frais annuels fermes tout compris pour chaque contrat et chaque année d'option sont ensuite résumés dans le Tableau A3.

Tableau A1 - Période du contrat

		A	B	C	D	E	F	G
	Fourchette annuelle des volumes	Facteur de pondération	Année 1 – Frais fermes tout compris par transaction par fourchette des volumes	Coefficient de pondération des prix de la fourchette des volumes (A × B)	Année 2 – Frais fermes tout compris par transaction par fourchette des volumes	Coefficient de pondération des prix de la fourchette des volumes (A × D)	Année 3 – Frais fermes tout compris par transaction par fourchette des volumes	Coefficient de pondération des prix de la fourchette des volumes (A × F)
1	**1 – 600 000**	0,10	**$**	**$**	**$**	**$**	**$**	$
2	**600 001 – 1 400 000**	0,50	**$**	**$**	**$**	**$**	**$**	$
3	**1 400 001 +**	0,40	**$**	**$**	**$**	**$**	**$**	**$**
4	Total des frais pondérés de transaction fermes tout compris (lignes 1 + 2 + 3)			**$**		**$**		**$**

Tableau A2 – Années d'option

		H	I	J	K	L
	Fourchette annuelle des volumes	Facteur de pondération	Année d'option 1 – Frais fermes tout compris par transaction par fourchette des volumes	Coefficient de pondération des prix de la fourchette des volumes (A × B)	Année d'option 2 – Frais fermes tout compris par transaction par fourchette des volumes	Coefficient de pondération des prix de la fourchette des volumes (A × D)
1	**1 – 600 000**	0,10	**$**	$	$	$
2	**600 001 – 1 400 000**	0,50	**$**	$	$	$
3	**1 400 001 +**	0,40	**$**	$	$	$
4	Total des frais pondérés de transaction fermes tout compris (lignes 1 + 2 + 3)			$		$

Tableau A3 – Total général – Sommaire des frais annuels de transaction fermes tout compris

FRAIS ANNUELS DE TRANSACTION FERMES TOUT COMPRIS						
	Catégorie	Année 1	Année 2	Année 3	Année d'option 1	Année d'option 2
1	Volumes prévus de DPA	1 170 000	1 320 000	1 410 000	1 520 000	1 560 000
2	Total des frais pondérés de transaction fermes tout compris (saisir les valeurs de la ligne 4 des tableaux A1 et A2)	**$**	**$**	**$**	**$**	**$**
3	**Frais annuels tout compris** (lignes 1 × 2)	**$**	**$**	**$**	**$**	**$**

B. <u>Frais de transaction d'effets retournés</u> :

Il s'agit des frais fermes tout compris de chaque transaction figurant dans le fichier de DPA envoyé par l'entrepreneur au receveur général, y compris les transactions retournées à l'entrepreneur par les institutions financières pertinentes ainsi que les transactions rejetées par l'entrepreneur lors des contrôles de validation initiaux des fichiers. Les frais fermes tout compris doivent tenir compte de toutes les exigences relatives au traitement et à l'établissement de rapports.

Directives

a) Les soumissionnaires devraient établir clairement les frais de transaction fermes tout compris pour chaque année dans le Tableau B1 (colonnes A, B, C, D et E).

Tableau B1 – Frais de transaction annuels tout compris des effets retournés

FRAIS ANNUELS DE TRANSACTION FERMES TOUT COMPRIS DES EFFETS RETOURNÉS						
		A	B	C	D	E
		Année 1	Année 2	Année 3	Année d'option 1	Année d'option 2
1	A – Volumes estimés d'effets retournés	19 000	22 000	23 000	25 000	26 000
2	B – Frais de transaction	$	$	$	$	$
3	**Frais annuels tout compris** (lignes 1 × 2)	$	$	$	$	$

C. Sommaire des frais :

Tableau C1 – Prix total évalué

		1	2	3	4	5
		Période du contrat Année 1	**Période du contrat Année 2**	**Période du contrat Année 3**	**Année d'option 1**	**Année d'option 2**
Description de l'élément		**Frais annuels tout compris**	**Frais annuels tout compris**	**Frais annuels tout compris**	**Frais annuels tout compris**	**Frais annuels tout compris**
A	**Frais des transactions de DPA (frais annuels tout compris indiqués dans le Tableau A3)**	**$**	**$**	**$**	**$**	**$**
B	**Frais des transactions des effets retournés (frais annuels tout compris indiqués dans le Tableau B1)**	**$**	**$**	**$**	**$**	**$**
Prix annuel évalué =		**$ (somme de la colonne 1)**	**$ (somme de la colonne 2)**	**$ (somme de la colonne 3)**	**$ (somme de la colonne 4)**	**$ (somme de la colonne 5)**
PRIX TOTAL ÉVALUÉ = (somme des prix annuels évalués des colonnes 1, 2, 3, 4 et 5)						_____**$**

PARTIE 4 - PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

1. Procédures d'évaluation

(a) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation technique.

(b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

1.1 Évaluation technique

1.1.1 Critères techniques obligatoires

Voir la pièce jointe 1 de la Partie 4.

1.2 Évaluation financière

1.2.1 Les données volumétriques comprises dans le barème de prix détaillé dans la pièce jointe 1 de la Partie 3 sont fournies uniquement aux fins de la détermination du prix évalué de chaque soumission. Elles ne doivent pas être considérées comme une garantie contractuelle.

1.2.2 Aux fins de l'évaluation des soumissions et de la sélection de l'entrepreneur ou, selon le cas, des entrepreneurs seulement, le prix évalué d'une soumission sera déterminé conformément au barème de prix détaillé dans la pièce jointe 1 de la Partie 3.

2. Méthode de sélection

2.1 Méthode de sélection - le prix évalué le plus bas

Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation obligatoires pour être déclarée recevable.

La soumission recevable ayant le prix évalué le plus bas sera recommandée pour attribution d'un contrat.

PIÈCE JOINTE 1 DE LA PARTIE 4
CRITÈRES TECHNIQUES

1.1.1 Critères techniques obligatoires

Les soumissions doivent satisfaire à tous les critères techniques obligatoires indiqués ci-dessous. Le soumissionnaire doit fournir la documentation nécessaire afin de démontrer qu'il se conforme à cette exigence.

Les soumissions qui ne satisfont pas à tous les critères techniques obligatoires seront déclarées irrecevables. Chaque critère technique obligatoire devrait être traité séparément.

Critères techniques obligatoires

L'expérience du soumissionnaire sera prise en considération aux fins de l'évaluation des critères techniques obligatoires énumérés ci-dessous.

Numéro	Critère technique obligatoire	Directives pour la préparation de la soumission
O1	Le soumissionnaire doit être un adhérent du Système de compensatin et de règlement automatisé (SCRA) ou un adhérent-correspondant de groupe affilié directement au SCRA. Le soumissionnaire doit fournir les documents nécessaires afin de démontrer qu'il respecte cette exigence.	Le soumissionnaire devrait fournir une preuve de son adhésion au SCRA. Il suffit de présenter un certificat d'adhésion, un numéro d'adhérent ou une lettre d'acceptation du SCRA.
O2	Le soumissionnaire doit fournir la description de deux (2) projets qu'il a menés à terme au cours des cinq (5) dernières années de la date de soumission, dans le cadre desquels il a dû traiter des opérations de DPA ou de JER d'au moins 850 000 $ par projet.	Pour chacun des projets, le soumissionnaire doit indiquer le nom, le titre, l'entreprise, l'adresse, l'adresse électronique et le numéro de téléphone de la personne-ressource, de même qu'une brève description du projet sur lequel a été fondée la relation.

PARTIE 5 - ATTESTATIONS

Pour qu'un contrat leur soit attribué, les soumissionnaires doivent fournir les attestations exigées. Le Canada déclarera une soumission non recevable si les attestations exigées ne sont pas remplies et fournies tel que demandé. Les soumissionnaires devraient inclure les attestations exigées dans la Section III de leur soumission.

Le Canada pourra vérifier l'authenticité des attestations fournies par les soumissionnaires pendant la période d'évaluation des soumissions (avant l'attribution d'un contrat) et après l'attribution du contrat. L'autorité contractante aura le droit de demander des renseignements supplémentaires pour s'assurer que les soumissionnaires respectent les attestations avant l'attribution d'un contrat. La soumission sera déclarée non recevable si on constate que le soumissionnaire a fait de fausses déclarations, sciemment ou non. Le défaut de respecter les attestations ou de donner suite à la demande de renseignements supplémentaires de l'autorité contractante aura pour conséquence que la soumission sera déclarée non recevable.

1. Attestations pour le Code de conduite - Attestations préalables à l'attribution du contrat

1.1 Les soumissionnaires doivent fournir, avec leur soumission ou le plus tôt possible après le dépôt de celle-ci, une liste complète de tous les individus qui sont actuellement administrateurs du soumissionnaire. Si la liste n'a pas été fournie à la fin de l'évaluation des soumissions, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Les soumissionnaires doivent fournir la liste des administrateurs avant l'attribution du contrat. Le défaut de fournir cette liste dans les délais prévus aura pour conséquence que la soumission sera déclarée non recevable.

L'autorité contractante peut, à tout moment, demander au soumissionnaire de fournir un formulaire de consentement dûment rempli et signé (Consentement à la vérification de l'existence d'un casier judiciaire - PWGSC-TPSGC 229) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/formulaires-forms-fra.html) pour toute personne inscrite sur la liste susmentionnée, et ce dans un délai précis. Le défaut de fournir le formulaire de consentement dans les délais prévus aura pour conséquence que la soumission sera déclarée non recevable.

2. Attestations additionnelles préalables à l'attribution du contrat

2.1 Attestations préalables à l'attribution du contrat

Les attestations comprises dans la pièce jointe 1 de la Partie 5, Attestations préalables à l'attribution du contrat, devraient être remplies et fournies avec la soumission, mais elles peuvent être fournies plus tard. Si l'une de ces attestations n'est pas remplie et fournie tel que demandé, l'autorité contractante en informera le soumissionnaire et lui donnera un délai afin de se conformer aux exigences. Le défaut de répondre à la demande de l'autorité contractante et de se conformer aux exigences dans les délais prévus aura pour conséquence le rejet de la soumission.

PIÈCE JOINTE 1 DE LA PARTIE 5
ATTESTATIONS PRÉALABLES À L'ATTRIBUTION DU CONTRAT

1.1 Programme de contrats fédéraux

1.1.1 Programme de contrats fédéraux- plus de 25 000 $ et moins de 200 000 $

Les fournisseurs qui sont assujettis au Programme de contrats fédéraux (PCF)et qui ont été déclarés entrepreneurs non admissibles par Ressources humaines et Développement des compétences Canada (RHDCC) n'ont plus le droit d'obtenir des contrats du gouvernement fédéral au-delà du seuil prévu par le Règlement sur les marchés de l'État pour les demandes de soumissions. Les fournisseurs peuvent être déclarés entrepreneurs non admissibles soit, parce que RHDCC a constaté leur non-conformité, ou, parce qu'ils se sont retirés volontairement du PCF pour une raison autre que la réduction de leur effectif à moins de 100 employés. Toute soumission présentée par un entrepreneur non admissible, y compris une soumission présentée par une coentreprise dont un membre est un entrepreneur non admissible, sera déclarée non recevable.

Le soumissionnaire ou, si le soumissionnaire est une coentreprise, le membre de la coentreprise atteste comme suit sa situation relativement au PCF :

Le soumissionnaire ou le membre de la coentreprise :

a. ( ) n'est pas assujetti au PCF, puisqu'il compte un effectif de moins de 100 employés permanents à plein temps, temps partiel et/ou temporaires ayant travaillé 12 semaines ou plus au Canada;

b. ( ) n'est pas assujetti au PCF, puisqu'il est un employeur réglementé en vertu de la Loi sur l'équité en matière d'emploi, L.C. 1995, ch. 44;

c. ( ) est assujetti aux exigences du PCF, puisqu'il compte un effectif de 100 employés ou plus permanents à plein temps, temps partiel et/ou employés temporaires ayant travaillé 12 semaines ou plus au Canada, mais n'a pas obtenu de numéro d'attestation de RHDCC, puisqu'il n'a jamais soumissionné pour des contrats de 200 000 $ ou plus;

d. ( ) n´a pas été déclaré entrepreneur non admissible par RHDCC et possède un numéro d'attestation valide, à savoir le numéro : _____.

Des renseignements supplémentaires sur le PCF sont offerts sur le site Web de RHDCC.

1.2 Attestation pour ancien fonctionnaire

Les contrats attribués à des anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du trésor sur les contrats avec des anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous.

Définitions

Aux fins de cette clause,

“ancien fonctionnaire” signifie tout ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques,* L.R., 1985, c. F-11, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être:

a) un individu;
b) un individu qui s’est incorporé;
c) une société de personnes constituée d’anciens fonctionnaires; ou
d) une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« période du paiement forfaitaire » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l’allocation de fin de services, qui se mesure de façon similaire.

« pension » signifie, dans le contexte de la formule de réduction des honoraires, une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension dans la fonction publique* (LPFP), L.R., 1985, ch. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17, à la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3, à la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada*, 1970, ch. R-10, et à la *Loi sur la pension de retraite de la Gendarmerie royale du Canada*, L.R., 1985, ch. R-11, à la *Loi sur les allocations de retraite des parlementaires*, L.R., 1985, ch. M-5, et à la partie de la pension versée conformément à la *Loi sur le Régime de pensions du Canada*, L.R., 1985, ch. C-8.

Ancien fonctionnaire touchant une pension

Est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension tel qu’il est défini ci-dessus ? **OUI ( ) NON ( )**

Si oui, le soumissionnaire doit fournir l’information suivante :

a) nom de l’ancien fonctionnaire, et
b) la date de cessation d’emploi dans la fonction publique ou de la retraite.

Programme de réduction des effectifs

Est-ce que le soumissionnaire est un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu des dispositions d’un programme de réduction des effectifs? **OUI ( ) NON ( )**

Si oui, le soumissionnaire doit fournir l’information suivante :

a) le nom de l’ancien fonctionnaire;
b) les conditions de l'incitatif versé sous forme de paiement forfaitaire;
c) la date de cessation d'emploi;
d) le montant du paiement forfaitaire;

e) le taux de rémunération qui a servi au calcul du paiement forfaitaire;
f) la période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines; et
g) le nombre et montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réduction des effectifs.

Pour tous les contrats attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peut être payé à un ancien fonctionnaire qui a reçu un paiement forfaitaire est limité à 5 000 $, incluant la taxe sur les produits et services ou la taxe de vente harmonisée.

Attestation

En déposant une soumission, le soumissionnaire atteste que l'information fournie par le soumissionnaire pour répondre aux exigences ci-dessus est exacte et complète.

1.3. Attestation du contenu canadien

1.3.1 Clause du Guide des CCUA A3050T, Définition du contenu canadien

1.3.2 Attestation du contenu canadien

Cet achat est conditionnellement limité aux services canadiens.

Sous réserve des procédures d´évaluation contenues dans la demande de soumissions, les soumissionnaires reconnaissent que seulement les soumissions accompagnées d´une attestation à l´effet que le service offert est un service canadien, tel qu´il est défini dans la clause A3050T, peuvent être considérées.

Le défaut de fournir cette attestation remplie avec la soumission aura pour conséquence que le service offert sera traité comme un service non-canadien.

Le soumissionnaire atteste que :

( ) le service offert est un service canadien tel qu´il est défini au paragraphe 2 de la clause A3050T.

PARTIE 6 - EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

1. Exigences relatives à la sécurité

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées:

(a) le soumissionnaire doit détenir une attestation de sécurité d'organisme valable, tel qu'indiquée à la Partie 7 - Clauses du contrat subséquent;

(b) les individus proposés par le soumissionnaire et qui doivent avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé doivent posséder une attestation de sécurité tel qu'indiquée à la Partie 7 - Clauses du contrat subséquent; et

(c) le soumissionnaire doit fournir le nom de tous les individus qui devront avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé.

2. On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir la cote de sécurité requise, demeure à l'entière discrétion de l'autorité contractante.

3. Pour de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le document « Exigences de sécurité dans les demandes de soumissions de TPSGC - Instructions pour les soumissionnaires (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-fra.html#a31) sur le site Web Documents uniformisés d'approvisionnement ministériels.

2. Capacité financière

Clause du Guide des CCUA A9033T(2012-07-16), Capacité financière

PARTIE 7 - CLAUSES DU CONTRAT SUBSÉQUENT

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

1. Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux, à l'Annexe A

1.1 Destination des Services

Travaux publics et Services gouvernementaux Canada
Région de la Capital National (Gatineau)
Phase III, Place du Portage
11 rue Laurier
Gatineau, Québec, K1A 0S5
Canada

2. Clauses et conditions uniformisées

Toutes les clauses et conditions identifiées dans le contrat par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

2.1 Conditions générales

2035 (2012-07-16), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

Le texte du paragraphe 4 de la section 41- Code de conduite et attestations - contrat, du document 2035 susmentionné est remplacé par ce qui suit :

Pendant toute la durée du contrat, l'entrepreneur doit diligemment tenir à jour la liste des noms de tous les individus qui sont administrateurs de l'entrepreneur et envoyer un avis écrit à l'autorité contractante chaque fois qu'il y a un changement d'administrateur. A la demande du Canada, l'entrepreneur doit également fournir les formulaires de consentement correspondants.

2.2 Conditions générales supplémentaires

4008 (2008-12-12), Renseignements personnels s'appliquent au contrat et en font partie intégrante.

3. Exigences relatives à la sécurité

3.1 Avant l'attribution d'un contrat, les conditions suivantes doivent être remplies:

1. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrées par la Direction de la sécurité industrielle canadienne de Travaux publics et Services gouvernementaux Canada.

2. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

3. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau PROTÉGÉ tant que la DSCI, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ B.

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

5. L'entrepreneur doit se conformer aux dispositions des documents suivants :

a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe C;

b) le Manuel de la sécurité industrielle (dernière édition).

4. Durée du contrat

4.1 Période du contrat

Les travaux doivent être réalisés à partir de la date d'attribution du contrat jusqu'au 31 mars 2016 inclusivement.

4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus (2) deux période(s) supplémentaire(s) de (1) une année (s) chacune, selon les mêmes conditions. L'entrepreneur accepte que pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de paiement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur au moins 30 jours civils avant la date d'expiration du contrat. Cette option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

4.3 Option de prolongation du contrat- Période de transition

L'entrepreneur reconnaît que la nature des services fournis en vertu du contrat exigent la continuité et qu'il peut être nécessaire d'ajouter une période de transition à la fin du contrat. L'entrepreneur accepte que le Canada puisse, à sa discrétion, prolonger le contrat d'une période de (4) quatre mois selon les mêmes conditions afin d'assurer la transition nécessaire. L'entrepreneur accepte que, durant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de Paiement.

L'autorité contractante avisera l'entrepreneur de la prolongation du contrat en lui faisant parvenir un avis écrit au moins 30 jours civils avant la date d'expiration du contrat. La prolongation sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

4.4. Résiliation avec avis de trente jours

1. Le Canada se réserve le droit de résilier à n'importe quel moment le contrat, en tout ou en partie, en donnant un avis écrit de trente (30) jours civils à l´entrepreneur.

2. Suite à cette résiliation, le Canada paiera uniquement les coûts engagés pour les services rendus et acceptés par le Canada avant la date de la résiliation. Malgré toute autre disposition du contrat, aucun autre coût résultant de la résiliation ne sera payé à l´entrepreneur.

5. Responsables

5.1 Autorité contractante

L'autorité contractante pour le contrat est:

Nom: Jocelyne C Gagnon
Titre: Spécialiste en contrat
Travaux publics et Services gouvernementaux Canada
Direction générale des approvisionnements
Direction: Division des Services des Affaires et de Consultation
Adresse: 11 rue Laurier
Phase III, 10C1
Ottawa, Ontario, K1A 0S5
Téléphone : (819) 956-0575
Télécopieur : (819) 956-2675
Courriel: jocelyne.c.gagnon@tpsgc-pwgsc.gc.ca

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

5.2 Chargé de projet

Le chargé de projet pour le contrat est:

Nom: _____
Titre: _____
Organisation: _____
Adresse: _____

Téléphone: ___- ___- ___
Télécopieur : ___- ___- ___
Courriel : _____

Le chargé de projet représente le ministère ou l'organisme pour lequel les travaux sont exécutés en vertu du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le chargé de projet; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. De tels changements peuvent être effectués uniquement au moyen d'une modification de contrat émise par l'autorité contractante.

5.3 Représentant de l'entrepreneur

Le Représentant de l'entrepreneur est:

6. Paiement

6.1 Base de paiement

6.1.1 Prix unitaire ferme

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé le prix unitaire ferme figurant à l'annexe "B", Base de paiement. Les droits de douane sont inclus et la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, s'il y a lieu.

Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés aux travaux.

L'entrepreneur doit aviser l'autorité contractante par écrit lorsque le coût total estimatif indiqué à la p. 1 du contrat est de 75 pour cent commis. La responsabilité totale du Canada envers l'entrepreneur en vertu du contrat ne doit pas dépasser le coût total estimatif à la page 1.

L'entrepreneur ne doit pas exécuter des travaux ou fournir des services qui auraient comme conséquence que la responsabilité totale du Canada dépasse l'approbation écrite de l'autorité contractante.

6.2 Méthode de paiement

6.2.1 Paiement mensuel

Clause H1008C (2008-05-12) du Guide des CCUA.

6.3 Clauses du guide des CCUA

A9117C (2007-11-30), T1204 - demande directe du ministère client
C2000C (2007-11-30), Taxes - entrepreneur établi à l'étranger

6.4 Vérification discrétionnaire des comptes

C0705C (2010-01-11), Vérification discrétionnaire des comptes

7. Instructions relatives à la facturation

L'entrepreneur doit soumettre ses factures conformément à l´article intitulé " Présentation des factures " des conditions générales. Les factures ne doivent pas être soumises avant que tous les travaux identifiés sur la facture soient complétés.

Chaque demande doit être appuyée par :

a) une copie de tout document tel qu´il est spécifié au contrat
b) une copie des factures, reçus, pièces justificatives pour tous les frais directs et pour tous les frais de déplacement et de subsistance;

c) le total des transactions Pré-Autorisées par mois
d) le total des transactions retournés par mois

Les demandes doivent être distribuées comme suit :

a) L'original et une (1) copie doivent être envoyés à l´adresse qui apparaît à la page 1 du contrat pour attestation et paiement.

b) Une (1) copie doit être envoyée à l´autorité contractante identifiée sous l´article intitulé "Responsables" du contrat.

8. Attestations

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

8.2 Clauses du guide des CCUA

A3060C (2008-05-12), Attestation du contenu canadien

9. Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur _____ et les relations entre les parties seront déterminées par ces lois.

10. Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.
a) les articles de la convention;
b) les conditions générales supplémentaires 4008 (2008-12-12);
c) les conditions générales 2035 (2012-07-16), Conditions générales - besoins plus complexes de services;
d) l'Annexe A, Énoncé des travaux;
e) l'Annexe B, Base de paiement;
f) l'Annexe C, Liste de vérification des exigences relatives à la sécurité; et
gi) la soumission de l'entrepreneur datée du _____

11. Ressortissants étrangers

11.1 Clause du guide des CCUA A2001C (2006-06-16), Ressortissants étrangers (entrepreneur étranger)

11.2 Clause du guide des CCUA A2000C (2006-06-16), Ressortissants étrangers (entrepreneur canadien)

11.3 Clause du guide des CCUA A9122C (2008-05-12), Protection et sécurité des données stockées dans des bases de données

12. Assurances

12.1 Clause du Guide des CCUA G1005C (2008-05-12), Assurances

ANNEXE A

ÉNONCÉ DES TRAVAUX

1.0 APERÇU

1.1 Introduction et contexte

En tant que receveur général du Canada, la ministre de Travaux publics et Services gouvernementaux Canada (TPSGC) gère les opérations du Trésor fédéral, notamment l'encaissement et le versement des fonds fédéraux dans le Trésor et à partir du Trésor. TPSGC regroupe la gestion des paiements et de la perception des recettes du gouvernement afin d'obtenir les tarifs les plus concurrentiels pour les services offerts par les institutions financières du Canada.

Bien que le receveur général perçoive les remises dans le cadre de nombreux accords, les exigences décrites dans le présent énoncé des travaux portent uniquement sur les services de débit préautorisé (DPA) et ne visent à remplacer aucun type de remises versées au receveur général, comme les espèces, les chèques, les cartes de crédit ou de débit, les transferts électroniques de fonds, ou les paiements de factures papier ou électroniques pour lesquels le receveur a conclu des contrats ou des ententes distinctes.

Un DPA est une transaction lancée par un ministère ou un organisme en vue d'effectuer des prélèvements d'un montant fixe ou variable, sur une base récurrente ou sporadique, directement à partir du compte bancaire d'un client. Les DPA sont autorisés par des accords écrits ou électroniques conclus entre le payeur et le ministère ou l'organisme gouvernemental qui fournit ce service.

Le cadre de traitement des DPA au moyen du système canadien de compensation et de règlement est établi conformément à la Règle H1 de l'Association canadienne des paiements (ACP), qui définit les procédures de traitement des DPA. Les normes et les règles du Système automatisé de compensation et de règlement de l'ACP mentionnées tout au long du présent énoncé des travaux, notamment les règles F5, H1 et A4 et la Norme 005, qui se trouvent le site Web de l'ACP à l'adresse suivante : http://cdnpay.ca/. L'entrepreneur doit se conformer aux règles de l'ACP, notamment en ce qui concerne les changements à venir.

À l'heure actuelle, six ministères et organismes utilisent le service de DPA. D'autres ministères souhaiteraient utiliser le service, mais ils devraient d'abord élaborer l'interface entre leurs systèmes et ceux du receveur général. À l'heure actuelle, les ministères actifs sont les suivants : Agence du revenu du Canada (ARC) pour l'impôt sur le revenu des particuliers et des entreprises; ministère des Anciens Combattants pour la prestation de soins à long terme aux anciens combattants hospitalisés à l'hôpital de Sainte-Anne-de-Bellevue; Agence de promotion économique du Canada atlantique pour leurs programmes; Banque du Canada pour les obligations d'épargne du Canada; Agence de développement économique du Canada pour les régions du Québec (ADECRQ) pour leurs programmes; ministère de la Défense nationale pour ses services. L'ARC et l'ADECRQ collaborent dans le cadre d'initiatives visant à étendre l'utilisation des DPA pendant la durée de la période de contrat. Ces initiatives ont été prises en considération lors de la définition des volumes prévus indiqués dans l'*Annexe A de l'Appendice 2 – Activités de DPA historiques et prévues*.

1.2 Objectif

Un contrat officiel est conclu avec un seul fournisseur de services, ci-après appelé l'entrepreneur, pour le traitement de tous les DPA en dollars canadiens, pour le compte du Canada.

1.3 Définitions

Veuillez vous reporter à l'*Annexe A, Appendice 1 – Définitions* pour obtenir la définition des termes utilisés dans le présent document.

1.3.1 Noms de fichiers

i. Fichier de DPA : Fichier envoyé par TPSGC à l'entrepreneur qui contient un lot de transactions de DPA. Ce fichier sera conforme à la Norme 005 de l'ACP.

ii. Fichier de débits préautorités retournés ou rejetés (DPAR) : Fichier envoyé par l'entrepreneur à TPSGC qui contient les DPA retournés reçus des institutions financières des payeurs ou les transactions rejetées dans le cadre de la validation initiale des fichiers de DPA effectuée par l'entrepreneur. Ce fichier sera conforme à la Norme 005 de l'ACP.

iii. Fichier de DPA de l'institution financière : Fichier envoyé par l'entrepreneur aux institutions financières adhérentes qui appliqueront les directives relatives au retrait. Ce fichier contient un lot de transactions de DPA et doit être conforme à la Norme 005 de l'ACP.

iv Fichier de DPAR de l'institution financière : Fichier envoyé par les institutions financières adhérentes à l'entrepreneur. Ce fichier contient un lot de DPA retournés envoyés par les institutions financières du payeur. Il sera conforme à la Norme 005 de l'ACP.

1.4 Ententes actuelles

Un contrat de DPA a été conclu avec une institution financière canadienne. Il s'étend jusqu'au 31 mars 2013 et est assorti d'une période option de trois mois, dans l'éventualité où une période de transition serait requise.

1.5 Renseignements statistiques

Des statistiques historiques et les volumes prévus sont fournis à l'*Annexe A, Appendice 2 – Activités de DPA historiques et prévues*. Bien que les prévisions concernant les volumes aient été établies avec le plus grand soin, rien ne garantit qu'elles se concrétiseront. Tous les calculs sont effectués de bonne foi à des fins d'information uniquement et ne doivent en aucun cas être interprétés comme une représentation des montants que le gouvernement du Canada percevra par l'intermédiaire du service de DPA.

2.0 EXIGENCES DE SERVICE DÉTAILLÉES

2.1 Exigences opérationnelles globales

L'entrepreneur devra fournir les services suivants :

i. Accepter les fichiers de DPA dans le format précisé par la Norme 005 de l'ACP à son centre de données. La méthode de présentation des fichiers de DPA est abordée plus en profondeur dans la section 2.3 « Échange de fichiers avec le receveur général » et le délai de présentation est précisé dans la section 2.4 « Délai de réception ».
ii. Effectuer la validation des fichiers comme il est indiqué dans la section 2.6 « Contrôle de validation », et traiter les transactions rejetées conformément à la section 2.7 « Procédure relative aux DPA rejetés ».
iii. Trier les transactions de débit valides et envoyer les fichiers de DPA aux institutions financières adhérentes qui appliqueront les directives relatives au retrait (ou qui transféreront ces transactions aux institutions financières sous-adhérentes avec lesquelles elles ont un lien). Ces fichiers doivent être envoyés au plus tard un jour ouvrable avant la date d'échéance afin de permettre la réalisation des débits à la date d'échéance. Dans l'éventualité où l'entrepreneur recevrait un fichier de DPA contenant des transactions dont la date d'échéance est passée, les fichiers de DPA des institutions financières contenant ces transactions doivent être envoyés immédiatement à l'entrepreneur.
iv. Accepter les fonds versés par les institutions financières du payeur pour toutes les transactions de débit transmises.
v. Traiter les DPA retournés conformément à la section 2.10 « Procédure relative aux DPA retournés ».
vi. Répondre aux demandes de renseignements du receveur général concernant les DPA, les DPA rejetés et les DPA retournés dans les délais prévus dans la section 2.12 « Suivis et demandes de renseignements ».

2.2 Adhésion

Le processus d'adhésion et de vérification sera exécuté par le ministère ou l'organisme demandeur du gouvernement, conformément aux règles de l'ACP. Il ne relève pas de l'entrepreneur.

2.3 Échange de fichiers avec le receveur général

Le Réseau de services de l'ACP doit obligatoirement être utilisé pour le transfert de fichiers. Pour des raisons de sécurité, la transmission de fichiers, à l'aide de cette méthode, se fait par relais de trames privées et est conforme à l'ensemble des règles et des normes de l'ACP (règles F5, H1 et A4, et Norme 005).

L'entrepreneur doit examiner de façon périodique la pertinence et le fonctionnement du mode de transmission et collaborer en apportant des changements aux normes, tel qu'il aura été convenu avec le receveur général. Si les nouvelles normes adoptées par les parties sont officiellement modifiées ou changées par l'émission d'une nouvelle version, l'entrepreneur doit faire de son mieux pour convenir d'un programme ou d'un calendrier et changer les directives et l'information dans le but de les rendre conformes aux nouvelles normes dans les plus brefs délais, et il doit collaborer afin que les changements soient apportés d'une manière commercialement raisonnable.

2.4 Délai de réception

Le receveur général doit transmettre les fichiers de DPA avant la date d'échéance conformément au code de fonctionnalité associé à l'institution financière du payeur (quatre [4] jours ou moins). Cependant, il est possible que les dates d'échéance de certaines des transactions contenues dans les fichiers de DPA soient passées depuis au plus 14 jours.

Chaque jour ouvrable, le receveur général doit transmettre à l'entrepreneur le fichier de DPA au plus tard à 9 h 30 (heure avancée de l'Est [HAE]) sauf pendant les jours où le bureau du receveur général est fermé. En cas de retard, le receveur général doit en aviser la personne-ressource responsable des opérations courantes de l'entrepreneur et lui communiquer l'heure prévue pour la transmission de ce fichier. Dans l'éventualité où des problèmes surviendraient et que le fichier ne pourrait pas être transmis, le receveur général communiquera avec l'entrepreneur, et les parties conviendront d'ententes mutuellement acceptables.

S'il n'a pas reçu les fichiers de DPA du receveur général avant 9 h 30 (HAE), l'entrepreneur doit communiquer avec la personne-ressource responsable des opérations courantes du receveur général pour se renseigner au sujet de ce retard. Au besoin, d'autres dispositions seront prises pour la transmission du fichier de DPA.

2.5 Distribution et traitement des fichiers et conservation des dossiers

L'entrepreneur doit :

i. Aux fins de suivi, conserver toutes les transactions de DPA et les transactions retournées ou rejetées pendant une période d'un an suivant la date d'échéance du DPA.
ii. Indiquer un numéro de création de fichier unique attribué selon un ordre séquentiel pour chaque fichier de DPA de l'institution financière et chaque fichier de DPAR aux fins de suivi et de rapprochement.

2.6 Contrôle de validation

Sur réception d'un fichier, l'entrepreneur doit effectuer rapidement les contrôles de validation. Chaque transaction doit être soumise à un contrôle de validation. L'entrepreneur doit rejeter uniquement les transactions qui échouent le contrôle de validation; il n'est pas nécessaire de rejeter le fichier en entier.

i. Effectuer la validation des fichiers de DPA, vérifier notamment :
    a) les transactions périmées (conformément aux exigences relatives à la date d'échéance énoncées dans la Norme 005 de l'ACP);
    b) la validité de la succursale et du numéro de l'institution financière, en fonction des mises à jour du fichier de l'institution financière fournies par l'ACP.
ii. Au besoin, effectuer la validation des fichiers de DPAR de l'institution financière, vérifier notamment :
    a) le demandeur autre que le gouvernement fédéral;
    b) le type de transaction invalide (seuls les codes de l'ACP seront acceptés);
    c) les transactions doubles dans les cas où la transaction de DPA d'origine a déjà été retournée;
    d) les transactions invalides où le numéro de repère d'effet du receveur général, le numéro de référence de paiement du receveur général ou le montant ne correspond pas à la transaction de DPA d'origine.

2.7 Procédure relative aux DPA rejetés

L'entrepreneur doit :

i. Procéder aux contrôles de validation des fichiers de DPA, comme il est prévu à la section 2.6 « Contrôle de validation ».

ii. Pour entreprendre le règlement des DPA rejetés, remplir un formulaire d'avis (ou un message SWIFT MT299), lequel doit être envoyé à la Banque du Canada au plus tard à 14 h 30 (HAE). Le montant indiqué dans l'avis ou le message MT299 est celui que la Banque du Canada enverra à l'entrepreneur par l'intermédiaire d'un paiement du Système de transfert de paiements de grande valeur (STPGV). La section 2.11.2 « Règlement des fichiers de DPAR » contient des renseignements supplémentaires sur le règlement des DPA rejetés. Les éléments de données devant figurer dans le formulaire d'avis de même que la mise en forme requise à l'égard du message MT299 se trouvent à la section 2.0 « Exigences concernant les avis de rejet ou de retour » figurant à l'*Annexe A – Appendice 3 – Exigences de la Banque du Canada relativement aux avis.*

iii. Retourner les transactions non enregistrées à TPSGC à l'aide du fichier de DPAR, conformément à la Norme 005 de l'ACP. Chaque fichier doit comprendre le numéro de repère d'effet et le numéro de référence de paiement du receveur général, et un numéro de création de fichier unique attribué par l'entrepreneur aux fins de suivi et de rapprochement. Ces fichiers doivent être envoyés par l'entrepreneur et reçus par le receveur général avant 19 h 45 (HAE), à la date du règlement. La valeur précisée dans les fichiers de DPAR doit correspondre au montant indiqué dans le formulaire d'avis ou le message MT299 ayant été envoyé à la Banque du Canada, conformément à l'étape (ii) de la présente section.

iv. Au besoin, inclure les DPA rejetés dans un fichier de DPAR contenant également des DPA retournés, ou les déclarer dans un fichier de DPA distinct.

2.8 Procédure relative au remplacement d'un fichier électronique

Si un fichier est illisible, l'entrepreneur doit, à la demande du receveur général, créer un nouveau fichier de DPAR puis le présenter de nouveau. Toute demande du receveur général doit être présentée dans les 15 jours ouvrables suivant la date où le fichier original a été transmis.

L'entrepreneur dispose d'au plus deux jours ouvrables pour présenter de nouveau un fichier de DPAR ou pour en créer un nouveau.

2.9 Flottant

L'entrepreneur doit verser au receveur général des intérêts sur le flottant pour tous les fonds dont la date de règlement est postérieure à la date à laquelle les fonds ont été versés à l'entrepreneur par l'institution financière du payeur. Le montant de ces intérêts sur le flottant sera calculé selon le taux précisé dans le protocole d'entente négocié entre les institutions financières adhérentes et le gouvernement du Canada. Actuellement, ce taux correspond au taux d'escompte (fixé par la Banque du Canada) moins le quart d'un point de pourcentage (0,25 %), même s'il est sujet à changement.

2.10 Procédure relative aux DPA retournés

L'entrepreneur doit :

i. se conformer aux règles de l'ACP concernant les DPA refusés notamment en raison d'insuffisance de provision, d'arrêt de paiement ou de fermeture de compte. Les effets doivent être retournés dans le délai précisé à la Règle A4 et conformément aux procédures établies à la Règle F5.

ii. Accepter les DPA retournés (fichiers de DPAR des institutions financières) transmis par les institutions financières du payeur au plus tard dans les 90 jours civils en ce qui concerne les DPA des particuliers ou les DPA liés à des transferts de fonds, ou dans les 10 jours civils en ce qui concerne les DPA des entreprises, suivant la date comptable figurant sur le relevé de compte, conformément aux règles de l'ACP.

iii. Procéder aux contrôles de validation des fichiers de DPAR des institutions financières, comme il est prévu à la section 2.6 intitulée « Contrôle de validation ».
iv. Se conformer à la Norme 005 de l'ACP relativement aux codes de rejet, au code d'identification du type d'enregistrement et à la disposition du fichier d'enregistrement.
v. Remplir un formulaire d'avis (ou un message SWIFT MT299), lequel doit être envoyé à la Banque du Canada au plus tard à 14 h 30 (HAE). Le montant indiqué dans l'avis ou le message MT299 est celui que la Banque du Canada enverra à l'entrepreneur par l'intermédiaire d'un paiement du STPGV. La section 2.11.2, intitulée « Règlement des fichiers de DPAR », contient des renseignements supplémentaires sur le règlement. Les éléments de données devant figurer dans le formulaire d'avis de même que la mise en forme requise à l'égard du message MT299 se trouvent à la section 2.0 « Exigences concernant les avis de rejet ou de retour » figurant à l'*Annexe A – Appendice 3 – Exigences de la Banque du Canada relativement aux avis.*
vi. Envoyer au receveur général les fichiers de DPAR contenant l'ensemble des transactions rejetées; le receveur général doit recevoir les fichiers avant 19 h 45 (HAE), à la date du règlement. La disposition de chaque fichier doit être conforme à celle établie à la Norme 005 de l'ACP, et chaque fichier doit comprendre le numéro de repère d'effet du receveur général, le numéro de référence de paiement du receveur général, de même que le numéro unique de création du fichier créé par l'entrepreneur aux fins de suivi ou de rapprochement. La valeur précisée dans les fichiers de DPAR doit correspondre au montant indiqué dans le formulaire d'avis ou le message MT299 ayant été envoyé à la Banque du Canada, conformément à l'étape (v) de la présente section.
vii. Transmettre les DPA retournés soit dans un fichier de DPAR contenant également des DPA rejetés, soit dans un fichier de DPAR distinct.
viii. Refuser, au nom du receveur général, tous les DPA retournés transmis par les membres adhérents après les délais établis dans les règles de l'ACP en matière de retours.

2.11 Règlement

2.11.1 Règlement des fichiers de DPA

i. L'entrepreneur doit amorcer le règlement et envoyer à la Banque du Canada, avant 15 h (HAE) à la date de la transaction de DPA, un message MT103 concernant un paiement du STPGV destiné au receveur général. La mise en forme requise à l'égard du message MT103 est indiquée à la section 3.0 intitulée « Spécifications des fichiers liés au message SWIFT MT103 » figurant à l'*Annexe A – Appendice 3 – Exigences de la Banque du Canada relativement aux avis*.
ii. Le paiement du STPGV doit être accompagné d'un formulaire d'avis ou d'un message SWIFT MT299. Le montant du paiement du STPGV doit correspondre à celui indiqué dans le formulaire d'avis ou dans le message MT299. Les éléments devant figurer dans le formulaire d'avis de même que la mise en forme requise à l'égard du message MT299 sont indiqués à la section 1.0 intitulée « Exigences concernant les avis de DPA » figurant à l'*Annexe A – Appendice 3 – Exigences de la Banque du Canada relativement aux avis.*
iii. Le montant indiqué dans le message MT103 concernant un paiement du STPGV doit correspondre à la valeur totale des fichiers de DPA. Les DPA retournés et rejetés ne devraient pas être déduits de la valeur des fichiers de DPA puisqu'ils sont réglés séparément (consulter la section 2.7 intitulée « Procédure relative aux DPA rejetés » et la section 2.10 intitulée « Procédure relative aux DPA retournés » pour en savoir davantage sur le règlement des DPA rejetés et des DPA retournés).

2.11.2 Règlement des fichiers de DPAR

La Banque du Canada amorcera le règlement et enverra à l'entrepreneur, avant 15 h (HAE) à la date de la transaction, un message MT103 concernant un paiement du STPGV destiné à l'entrepreneur. La Banque du Canada fournira les renseignements obligatoires et indiquera *« DPA retourné »* dans la zone réservée à cet effet. Le montant du paiement du STPGV envoyé par la Banque du Canada doit correspondre à celui que l'entrepreneur a indiqué dans le formulaire d'avis ou le message MT299 décrit à la partie (v) de la section 2.10 intitulée « Procédure relative aux DPA retournés » ou à la partie (ii) de la section 2.7 intitulée « Procédure relative aux DPA rejetés ».

2.12 Suivis et demandes de renseignements

L'entrepreneur doit, à la demande du receveur général, répondre à toute demande de renseignements et fournir des précisions à l'égard d'une transaction de DPA dans un délai de cinq jours ouvrables. S'il n'a pas obtenu de réponse après ce délai, le receveur général peut acheminer la demande de renseignements à un échelon supérieur de l'organisation de l'entrepreneur. Toute demande de renseignements liée à un suivi doit comprendre un numéro de repère original de TPSGC; ce numéro doit être mentionné dans toutes les réponses.

2.13 Rapports

Le receveur général satisfera à ses propres exigences en matière d'établissement de rapports au moyen des fichiers de DPA et de DPAR envoyés par l'entrepreneur.

2.14 Délai de réponse

L'entrepreneur doit répondre à toute demande de renseignements concernant la facturation dans un délai de sept jours civils. Le délai pour répondre à toutes les autres demandes de renseignements présentées par le receveur général par téléphone ou par courriel est de deux heures.

3.0 ACTIVITÉS TRANSITOIRES

3.1 Mise en œuvre du service

i. Les activités de mise en œuvre doivent commencer dans les cinq jours ouvrables suivant la date de l'attribution du contrat. Ces activités comprennent ce qui suit :
   a) tenir, dans les trois jours ouvrables suivant un avis envoyé par le receveur général, des réunions ou des conférences téléphoniques, selon le cas, entre les équipes de la haute direction, des opérations et du soutien technique et le receveur général afin de garantir le bon déroulement la mise en œuvre et la continuité des activités;
   b) achever un plan de transition et le présenter au receveur général dans les quatorze jours civils suivant la date de l'attribution du contrat;
   c) entreprendre une phase de transition dont la durée ne doit pas dépasser 90 jours civils et qui doit comprendre ce qui suit :
      1. phase d'installation de l'entrepreneur (exigences techniques),
      2. contrôles de validation et mises en forme conformément à l'énoncé des travaux,
      3. présentation des détails relatifs aux transactions et aux fichiers de DPA et de DPAR conformément à l'énoncé des travaux,

4. exigences en matière d'essais à l'égard de la transmission des fichiers de DPA et de DPAR auprès du receveur général,
5. disponibilité aux fins de mise à l'essai des fichiers électroniques dans un environnement d'essai,
6. une fois l'approbation du receveur général reçue, passage de la transmission électronique à l'environnement de production,
7. présentation au receveur général d'un plan d'urgence en ce qui concerne les points d'échange et les délais,
8. établissement de la liaison avec la Banque du Canada afin de mettre la dernière main aux ententes de règlement,
9. toute autre exigence conformément à l'énoncé des travaux;

ii. L'entrepreneur doit, dans les quatorze jours civils suivant la date d'attribution du contrat, fournir une liste contenant les coordonnées (nom, numéro de téléphone, adresse électronique, numéro de télécopieur et adresse postale, s'il y a lieu) du chef d'équipe, du gestionnaire de comptes et du gestionnaire de projet devant assurer la gestion des problèmes liés à l'administration du contrat visé, celles des personnes-ressources de deuxième et de troisième niveaux, de même que les délais d'exécution maximaux auxquels on peut s'attendre.

La liste des coordonnées du personnel autorisé présentée par l'entrepreneur doit comprendre les personnes-ressources liées aux activités quotidiennes, aux questions de sécurité d'accès, au soutien informatique et technique pour la période de transition et les activités courantes, ainsi qu'à l'envoi de la facturation mensuelle du receveur général pour les services rendus.

3.2 Élimination progressive de la prestation des services (période de transition)

L'entrepreneur doit, à la fin de la phase opérationnelle du contrat ou à la réception d'un avis envoyé par l'autorité contractante signifiant notre intention de mettre fin au contrat, continuer de fournir le même niveau de services à un volume réduit, selon les mêmes modalités et tarifs prévus au contrat, pendant une période ne dépassant pas quatre mois afin de régler toutes les transactions. La période totale du contrat comprend la phase opérationnelle, mais pas la période d'élimination progressive (période de transition).

L'entrepreneur convient également qu'il devra fournir au responsable du projet, si celui-ci en fait la demande à la fin de la période d'élimination progressive (période de transition), un fichier de données électroniques contenant tous les renseignements recueillis pendant la période du contrat.

4.0 AUTRES EXIGENCES

4.1 Plan d'urgence et de reprise après sinistre

Comme il est indiqué dans la *Pièce jointe 1 de l'Annexe C – Exigences en matière de sécurité de la TI*, l'entrepreneur doit disposer d'un plan d'urgence et de reprise après sinistre officiel en cas de panne d'électricité, d'incendie, d'interruption de travail ou de toute autre situation qui peut entraîner une interruption de la prestation du service. Dans de telles situations, l'entrepreneur mettra tout en œuvre pour maintenir des communications normales avec le receveur général en utilisant d'autres moyens qui auront été convenus entre les deux parties. Même en situation d'urgence, le format des fichiers doit demeurer conforme à la Norme 005 de l'ACP.

4.2 Sécurité et protection des renseignements personnels

L'entrepreneur doit s'assurer de respecter les exigences en matière de sécurité des technologies de l'information précisées dans l'*Annexe C* et dans la *Pièce jointe 1 de l'Annexe C – Exigences en matière de sécurité de la TI*.

4.3 Langue des services

L'entrepreneur doit fournir les services dans les deux langues officielles du Canada, soit en français et en anglais. La *Loi sur les langues officielles* de même que les politiques et les publications du Secrétariat du Conseil du Trésor sont disponibles sur les sites Web suivants :

http://lawslois.justice.gc.ca/fra/lois/O3.01/
http://www.tbs-sct.gc.ca/pol/index-fra.aspx

4.4 Modification des normes de paiement pendant le contrat

Comme il est précisé dans la revue annuelle de 2011 de l'ACP, les membres du conseil d'administration de l'ACP ont convenu que la norme ISO 20022 constituerait l'orientation future en matière de normes au Canada. L'objectif consiste à remplacer l'ensemble des normes utilisées aux fins des paiements réglés et établis par l'intermédiaire de l'ACP (y compris la Norme 005 liée au transfert automatisé de fonds et le STPGV) par la norme ISO 20022. Le receveur général souhaite ainsi être l'un des premiers à adopter cette nouvelle norme. Si la norme ISO 20022 devait être mise en œuvre pendant la durée du présent contrat, l'entrepreneur devrait, à la demande du receveur général, accepter d'envoyer les fichiers de transfert automatisé de fonds et les fichiers du STPGV dans ce nouveau format.

4.5 Modification du processus d'établissement de rapports et de règlement pendant le contrat

En raison de changements apportés au système interne, à un moment donné pendant la durée du contrat, le receveur général peut demander que le processus d'établissement de rapports et de règlement soit modifié en ce qui concerne les transactions de DPAR. Si ces modifications devaient être mises en œuvre, l'entrepreneur ne serait plus obligé d'envoyer un formulaire d'avis ou un message MT299 à la Banque du Canada, ni de transmettre par la suite les fichiers de DPAR connexes au receveur général. On demanderait plutôt à l'entrepreneur d'envoyer les fichiers de DPAR au receveur général avant 8 h 30 (HAE) afin que la Banque du Canada lui envoie un paiement le jour même (sous forme d'un message MT103 concernant un paiement du STPGV).

ANNEX A – APPENDICE 1
DÉFINITIONS

Date d'échéance : Date à laquelle le payeur autorise qu'on retire des fonds de son compte.

Date de présentation du fichier : Jour ouvré au cours duquel le fichier de DPA est fourni à l'entrepreneur.

Date de la transaction de DPA : Date à laquelle les fonds ont été débités du compte du payeur.

Date de règlement : Aux fins du règlement de fichiers de DPA, date à laquelle le receveur général reçoit la valeur à la Banque du Canada. Aux fins du règlement de fichiers de DPAR, date à laquelle l'entrepreneur reçoit la valeur à l'égard des DPA rejetés et des DPA retournés.

DPAR : Transactions de débit préautorisé rejetées ou retournées.

Fichier de l'institution financière : Répertoire électronique des institutions financières et de leurs succursales tenu à jour par l'ACP.

Noms de fichiers (fichier de DPA, fichier de DPAR, fichier de DPA de l'institution financière, fichier de DPAR de l'institution financière) : Veuillez consulter les définitions figurant au point 1.3 de l'Annexe A.

Jour ouvrable : Toute journée du lundi au vendredi, sauf les jours fériés nationaux, comme le précisent les définitions de l'ACP. Les jours fériés régionaux et municipaux sont considérés comme des jours ouvrables.

Numéro de repère d'effet : Numéro à 22 caractères fourni par le receveur général que l'entrepreneur indique pour toutes les transactions dans un fichier de DPA. Le numéro de repère d'effet original est également indiqué pour toutes les transactions dans un fichier de DPAR envoyé au receveur général par l'entrepreneur.

Numéro de référence de paiement : Numéro de référence attribué par le Système normalisé des paiements aux fins de référence interne par le receveur général et l'initiateur; un numéro est attribué pour chaque transaction de DPA.

Payeur : Personne ou organisation qui préautorise le retrait de fonds directement de son compte bancaire.

Rejet : Transaction qui échoue aux contrôles de validation initiaux effectués par l'entrepreneur et qui est retournée au receveur général.

Relais de trame : Protocole de commutation par paquets aux fins de connexion d'appareils sur un réseau étendu. Ce type de connexion de lignes est utilisé par les services de réseaux de l'ACP afin de garantir un niveau de sécurité maximal.

Retour : Transaction retournée par l'institution financière du payeur pour des raisons liées aux règles et aux normes de l'ACP.

SWIFT : Society for Worldwide Interbank Financial Telecommunication.

Système de transfert de paiements de grande valeur (STPGV) : Système de transfert de paiement en temps réel appartenant à l'ACP et utilisé par celle-ci aux fins de traitement des paiements de grande valeur et d'échange électronique de messages de paiement entre les participants au STPGV.

Système normalisé des paiements (SNP) : Système de trésorerie géré par le receveur général.

ANNEXE A – APPENDICE 2
HISTORIQUE ET PRÉVISIONS RELATIVEMENT AUX ACTIVITÉS DE DPA

1.0 Historique des volumes et des valeurs des DPA pour les exercices allant de 2009-2010 à 2011-2012

	Transactions		Retours	
Exercice 2009-2010	**Volume**	**Valeur (en dollars)**	**Volume**	**Valeur (en dollars)**
2009-04	64,617	124,873,663	1,101	540,337
2009-05	66,660	120,866,061	1,000	623,494
2009-06	115,903	264,149,061	1,647	2,577,659
2009-07	71,694	126,854,165	1,221	623,576
2009-08	68,192	115,082,902	1,195	654,953
2009-09	113,169	255,918,679	1,751	5,395,789
2009-10	73,364	123,230,039	1,301	637,198
2009-11	70,421	119,238,313	1,270	746,734
2009-12	115,176	266,064,355	1,826	4,420,346
2010-01	70,613	125,294,908	1,604	617,228
2010-02	67,333	120,713,766	1,298	525,918
2010-03	117,450	258,755,616	1,928	2,212,875
Totaux	***1,014,592***	***2,021,041,528***	***17,142***	***19,576,107***
Exercice 2010-2011				
2010-04	73,186	128,946,692	1,063	614,227
2010-05	69,241	122,532,163	1,419	591,318
2010-06	113,949	250,026,930	1,734	2,152,251
2010-07	74,585	123,924,759	1,267	606,417
2010-08	72,987	122,277,983	1,297	674,316
2010-09	111,165	228,799,901	1,806	3,391,125
2010-10	73,933	123,206,138	1,305	683,228
2010-11	75,975	126,593,381	1,350	589,853
2010-12	116,048	236,699,604	1,711	1,902,482
2011-01	73,455	128,195,244	1,507	607,596
2011-02	70,960	119,308,440	1,234	463,778
2011-03	110,754	235,145,041	1,913	1,557,040
Totaux	***1,036,238***	***1,945,656,276***	***17,606***	***13,833,631***

Exercice 2011-2012	Transactions		Retours	
	Volume	Valeur (en dollars)	Volume	Valeur (en dollars)
2011-04	72,751	122,701,187	1,308	802,587
2011-05	74,839	129,126,127	1,399	711,492
2011-06	111,219	228,204,431	1,795	2,013,529
2011-07	74,500	119,689,442	1,319	790,791
2011-08	77,144	126,020,107	1,537	667,638
2011-09	114,526	234,199,058	1,691	2,525,593
2011-10	74,791	119,614,993	1,239	602,103
2011-11	74,109	122,796,814	1,277	501,698
2011-12	114,039	233,089,821	1,648	2,363,672
2012-01	75,654	131,786,652	1,355	732,220
2012-02	72,760	121,062,244	1,209	490,960
2012-03	111,011	224,790,982	1,539	1,935,844
Totaux	***1,047,343***	***1,913,081,858***	***17,316***	***14,138,127***

2.0 Volumes prévus

Période du contrat	Transactions	Retours
2013/2014	1 170 000	19 000
2014/2015	1 320 000	22 000
2015/2016	1 410 000	23 000
Année d'option 1 – 2016-2017	1 520 000	25 000
Année d'option 2 – 2017-2018	1 560 000	26 000

ANNEXE A – APPENDICE 3
EXIGENCES DE LA BANQUE DU CANADA RELATIVEMENT AUX AVIS

1.0 Exigences concernant les avis de DPA

1.1 Éléments de données devant figurer dans les avis relatifs aux fichiers de DPA

a) titre du document : « DPA – Renseignements sur la valeur du règlement »;
b) nom de l'institution financière;
c) date du règlement;
d) renseignements sur chaque fichier de DPA compris dans le règlement, notamment :
    i. la date d'échéance;
    ii. le numéro d'identification de l'initiateur;
    iii. le numéro de création du fichier;
    iv. le nombre de paiements par carte de débit;
    v. le montant du paiement.
e) valeur totale du règlement :
    i. cette valeur doit correspondre à la somme des montants des paiements de chaque fichier de DPA figurant au point (d), de même qu'au montant indiqué dans le message MT103 concernant un paiement du STPGV envoyé à la Banque du Canada;
f) coordonnées de l'expéditeur.

1.2 Spécifications des fichiers liés au message SWIFT MT299

Code de la zone SWIFT	Nom de la zone SWIFT	Renseignements exigés par la Banque du Canada
20	Client Reference	PAD Settlement
21	Related Reference	Receiver General
32A	Value date, Currency, Settlement Amount	
79	Narrative	ATTN: Payment and Settlement Operations Government PAD Settlement Settlement Date: YYYY-MM-DD Details of Settlement Value: i. la date d'échéance; ii. le numéro d'identification de l'initiateur; iii. le numéro de création du fichier; iv. le nombre de paiements par carte de débit; v. le montant du paiement. Total Settlement Value: en dollars canadiens Coordonnées de la personne-ressource Numéro de téléphone Poste

2.0 Exigences concernant les avis de rejet ou de retour

2.1 Éléments de données devant figurer dans les avis relatifs aux fichiers de DPAR

a) titre du document : « DPA – Renseignements sur les rejets et les retours »;
b) nom de l'institution financière;
c) date de présentation du fichier rejeté ou retourné;
d) renseignements sur chaque fichier de DPAR compris dans le règlement, notamment :
    i. le numéro de création du fichier;
    ii. le nombre de paiements par carte de débit;
    iii. le montant du paiement.
e) Valeur totale des rejets et des retours;
    i. cette valeur doit correspondre à la somme des montants des paiements de chaque fichier de DPAR figurant au point (d), qui représente le montant que la Banque du Canada enverra à l'entrepreneur par l'intermédiaire du STPGV à la date de présentation du fichier rejeté ou retourné;
f) coordonnées de l'expéditeur.

2.2 Spécifications des fichiers liés au message SWIFT MT299

Code de la zone SWIFT	Nom de la zone SWIFT	Renseignements exigés par la Banque du Canada
20	Client Reference	PAD Return
21	Related Reference	Receiver General
32A	Value date, Currency, Settlement Amount	
79	Narrative	ATTN: Payment and Settlement Operations Government PAD Return / Reject Settlement Date: YYYY-MM-DD Details of Settlement Value: i. le numéro de création du fichier; ii.le nombre de paiements par carte de débit; iii. le montant du paiement. Total Return / Reject Value: en dollars canadiens Coordonnées de la personne-ressource Numéro de téléphone Poste

3.0 Spécifications des fichiers liés au message SWIFT MT103

Code de la zone SWIFT	Nom de la zone SWIFT	Renseignements exigés par la Banque du Canada
20	Client Reference	Govt PAD
23B	Bank Opération Code	CRED
32A	Value date, Currency, Settlement Amount	
50A	Ordering Customer	Code d'identification de la banque de l'entrepreneur (BIC)
57A	Account with Institution	Code d'identification de la Banque du Canada (BIC)
59	Beneficiary Customer	Numéro de compte du receveur général auprès de la Banque du Canada Receveur général
72	Bank to Bank Information	/ACC/560 : ou /BNF/560 : ou /REC/560 :

ANNEXE B

BASE DE PAIEMENT

Période du contrat : La période du contrat commence à la date de l'attribution du contrat et se termine le 31 mars 2016.

Pendant la durée du contrat, l'entrepreneur sera payé selon les modalités ci-après en contrepartie des travaux accomplis conformément au contrat. Les droits de douane sont compris et la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, le cas échéant.

1.0 Frais de transaction de DPA

Il s'agit des frais de transaction fermes tout compris de chaque débit figurant dans le fichier de DPA transmis par le receveur général, lequel fichier passe l'étape initiale de validation de l'entrepreneur et est finalement joint aux fichiers de DPA transmis aux institutions financières afin d'effectuer le débit à partir des comptes des clients. Les frais de transaction tout compris tiendraient compte de toutes les exigences relatives au traitement et à l'établissement de rapports.

		A	B	C	D	E
	Volumes	Frais fermes tout compris de transactions de DPA Année 1	Frais fermes tout compris de transactions de DPA Année 2	Frais fermes tout compris de transactions de DPA Année 3	Frais fermes tout compris de transactions de DPA Année d'option 1	Frais fermes tout compris de transactions de DPA Année d'option 2
1	1 – 600 000	$	$	$	$	$
2	600 001 – 1 400 000	$	$	$	$	$
3	1 400 001 +	$	$	$	$	$

Si une période de transition est nécessaire, les frais s'y rapportant correspondront aux taux qui s'appliquent au moment où l'avis concernant la période de transition est envoyé.

2.0 Frais de transaction d'effets retournés :

Il s'agit des frais fermes tout compris de chaque transaction figurant dans le fichier de DPA envoyé par l'entrepreneur au receveur général, y compris les transactions retournées à l'entrepreneur par les institutions financières pertinentes ainsi que les transactions rejetées par l'entrepreneur lors des contrôles de validation initiaux des fichiers. Ces frais unitaires tiendront compte de toutes les exigences relatives au traitement et à l'établissement de rapports.

	Frais fermes tout compris pour l'année 1	Frais fermes tout compris pour l'année 2	Frais fermes tout compris pour l'année 3	Frais fermes tout compris pour l'année d'option 1	Frais fermes tout compris pour l'année d'option 2
Frais de transaction fermes tout compris relatifs aux effets retournés	$	$	$	$	$

Si une période de transition est nécessaire, les frais s'y rapportant correspondront aux taux qui s'appliquent au moment où l'avis concernant la période de transition est envoyé.

2.1 Estimation du coût total - Période du contrat : _____ $. Les droits de douane sont compris et la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, le cas échéant.

2.2 Estimation du coût total - Option de prolongatin du contrat (Du ____ Au ____): _____$. Les droits de douane sont compris et la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, le cas échéant.

ANNEXE C

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Voir ci-joint

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN891130776
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Public Works and Government Services Canada	BAD / ABCB
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

To provide Pre-Authorized Debit (PAD) services as detailed in the SOW, as well as to include a SRCL and IT Technical Requirements into the Contract.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑ Not releasable / À ne pas diffuser ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	All NATO countries / Tous les pays de l'OTAN ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	No release restrictions / Aucune restriction relative à la diffusion ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☐ PROTECTED B / PROTÉGÉ B ☑ PROTECTED C / PROTÉGÉ C ☐ CONFIDENTIAL / CONFIDENTIEL ☐ SECRET / SECRET ☐ TOP SECRET / TRÈS SECRET ☐ TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐ NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐ NATO SECRET / NATO SECRET ☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	PROTECTED A / PROTÉGÉ A ☐ PROTECTED B / PROTÉGÉ B ☐ PROTECTED C / PROTÉGÉ C ☐ CONFIDENTIAL / CONFIDENTIEL ☐ SECRET / SECRET ☐ TOP SECRET / TRÈS SECRET ☐ TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN891130776
Security Classification / Classification de sécurité UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

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

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET – SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN891130776
Security Classification / Classification de sécurité UNCLASSIFIED

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

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

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

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

Pièce jointe 1 de l'Annexe C : Exigences en matière de sécurité de la Technologie de l'information (TI)

Le fournisseur de services doit démontrer que tout système de TI et/ou application utilisé pour assurer la prestation du service de débit pré-autorisé est conforme aux présentes exigences de référence en matière de sécurité de la TI. Dans la mesure où cela s'applique aux solutions de débit pré-autorisé proposées et le responsable du projet l'exige, le fournisseur de services doit également démontrer la conformité de ces systèmes et applications aux exigences supplémentaires. Toutefois, le responsable du projet pourra considérer certaines d'entre elles comme non pertinentes par rapport à la solution de débit pré-autorisé proposée.

1.1 Politique et procédures (PP)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à la politique et aux procédures et s'appliquant au service de débit pré-autorisé, tous domaines de la sécurité de la TI confondus.

Tableau C-1 : Liste des exigences en matière de politique et de procédures

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
PP-01	POLITIQUE ET PROCÉDURES	• Le fournisseur de services prépare, publie, révise et met à jour, au moins une fois par année, une politique officielle écrite traitant des objectifs, de l'étendue, des rôles, des responsabilités, de l'engagement de la direction, de la coordination entre les entités du fournisseur de services et de la conformité relativement à chacun des éléments suivants : o contrôle d'accès; o sensibilisation et formation à la sécurité; o vérification et responsabilisation; o évaluation de la sécurité et autorisation; o gestion de la configuration; o planification d'urgence; o identification et authentification; o réaction aux incidents; o maintenance du système; o protection des supports d'information; o domaine physique et environnemental; o planification de la sécurité; o sécurité du personnel; o évaluation des risques; o système et acquisition de services;	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ isolement de la fonction de sécurité; ○ intégrité du système et de l'information. • Le fournisseur de services prépare, publie, révise et met à jour, au moins une fois par année, des procédures officielles écrites visant à faciliter la mise en œuvre des politiques et des contrôles connexes relativement aux éléments suivants : ○ contrôle d'accès; ○ sensibilisation et formation à la sécurité; ○ vérification et responsabilisation; ○ évaluation de la sécurité et autorisation; ○ politique de gestion de la configuration et contrôles associés; ○ planification d'urgence, y compris un cycle de vérification du programme des plans d'urgence qui servira de base à la préparation de rapports réguliers au Secrétariat du Conseil du Trésor (SCT); ○ identification et authentification; ○ réaction aux incidents, y compris la hausse des niveaux de préparation en cas de situations d'urgence et de situations de menace accrue contre la sécurité des TI, conformément à la *Norme opérationnelle de sécurité : niveaux de préparation des installations du gouvernement fédéral* et à la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, toutes deux établies par le SCT; ○ maintenance du système d'information; ○ protection des supports d'information; ○ domaine physique et environnemental; ○ planification de la sécurité; ○ sécurité du personnel; ○ évaluation des risques; ○ système et acquisition de services; ○ protection du système et des communications; ○ intégrité du système et de l'information.	✓	

1.2 Contrôle d'accès (AC)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine du contrôle d'accès et s'appliquant au service de débit pré-autorisé.

Tableau C-2 : Liste des exigences en matière de contrôle d'accès

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AC-02	GESTION DES COMPTES	• Le fournisseur de services gère les comptes du système d'information : ○ désignation des types de compte (individuel, de groupe, de système, d'application, d'invité [ou anonyme], temporaire); ○ établissement des conditions d'inscription dans un groupe; ○ identification des utilisateurs autorisés du système d'information et détermination des privilèges d'accès; ○ demande des autorisations nécessaires pour toute demande de création de compte; ○ création, activation, modification, désactivation et suppression de comptes; ○ autorisation et surveillance de l'utilisation des comptes d'invité, anonymes et temporaires; ○ envoi d'un avis aux gestionnaires de comptes une fois que les comptes temporaires ne sont plus nécessaires, à la suite du départ ou de la mutation des utilisateurs du système d'information ou à la suite d'une modification de l'utilisation du système d'information, du besoin de connaître ou du besoin de partager; ○ désactivation des comptes temporaires devenus inutiles et des comptes des utilisateurs ayant quitté leur emploi ou ayant été mutés; ○ attribution d'accès au système en fonction d'une autorisation d'accès valide, de l'utilisation prévue du système et d'autres paramètres exigés par le fournisseur de services ou les missions ou fonctions opérationnelles associées; ○ examen des comptes au moins une fois par année.	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AC-02-01	GESTION DES COMPTES	• Le fournisseur de services : ○ utilise des mécanismes automatisés pour appuyer la gestion des comptes du système d'information; ○ exige que le système ferme automatiquement la session des utilisateurs après 15 minutes d'inactivité; ○ détermine l'heure de la journée et la durée d'utilisation normales pour les comptes du système d'information; ○ assure une surveillance en vue de repérer toute utilisation atypique des comptes du système d'information; ○ signale toute utilisation atypique à ses représentants désignés; ○ crée et administre les comptes d'utilisateurs privilégiés conformément à un plan d'accès qui structure les privilèges touchant le système d'information et le réseau en fonction des rôles; ○ suit et surveille les attributions de rôles privilégiés. • De manière automatique, le système d'information : ○ ferme les comptes temporaires et d'urgence au terme d'une période indiquée dans un document officiel et propre à chaque type de compte; ○ désactive les comptes inactifs au terme d'une période indiquée dans un document officiel; ○ vérifie la création, la modification, la désactivation et la fermeture des comptes et avise les personnes concernées, au besoin.		✓ ✓
AC-03	APPLICATION DE L'ACCÈS	• Le système d'information applique les autorisations approuvées relativement à l'accès logique au système conformément à la politique applicable.	✓	
AC-03-01	APPLICATION DE L'ACCÈS	• Le système d'information applique une politique de contrôle d'accès discrétionnaire qui : ○ permet aux utilisateurs de préciser et de gérer le partage par des personnes nommées ou des groupes de personnes, ou les deux;		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ limite la propagation des droits d'accès; ○ inclut ou exclut l'accès jusqu'au niveau de l'utilisateur unique.		
AC-04	APPLICATION DU FLUX DE L'INFORMATION	• Le système d'information applique les autorisations approuvées pour contrôler le flux de l'information au sein du système et entre les systèmes interconnectés conformément à la politique applicable.	✓	
AC-05	SÉPARATION DES TÂCHES	• Le fournisseur de services : ○ sépare les tâches des personnes, au besoin, afin de prévenir les actes malveillants non liés à la collusion; ○ met par écrit la séparation des tâches; ○ met en œuvre la séparation des tâches par l'attribution d'autorisations d'accès au système d'information.	✓	
AC-06	DROITS D'ACCÈS MINIMAUX	• Le fournisseur de services recourt au concept des droits d'accès minimaux, c'est-à-dire qu'il accorde aux utilisateurs (et aux processus agissant au nom des utilisateurs) seulement les accès autorisés dont ils ont besoin pour accomplir les tâches attribuées conformément aux missions et aux fonctions opérationnelles du fournisseur de services.	✓	
AC-06-01	DROITS D'ACCÈS MINIMAUX	• Le fournisseur de services autorise explicitement l'accès aux fonctions de sécurité mises en place dans le matériel, les logiciels et les micrologiciels ainsi qu'aux renseignements liés à la sécurité. • Le fournisseur de services exige que les titulaires de comptes dans le système d'information (ou les titulaires de rôles) ayant accès aux fonctions de sécurité ou aux renseignements liés à la sécurité utilisent des comptes ou rôles non privilégiés pour accéder à d'autres fonctions du système. Il vérifie également toute utilisation des comptes ou rôles privilégiés pour accéder à ces autres fonctions. • Le fournisseur de services limite l'autorisation d'accès aux comptes de superutilisateurs dans le système d'information au personnel affecté à l'administration du système.		✓ ✓ ✓
AC-07	TENTATIVES	• Le système d'information applique une limite de TROIS tentatives	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	INFRUCTUEUSES D'OUVERTURE DE SESSION	d'ouverture de session infructueuses consécutives par un utilisateur pendant une journée. • De manière automatique, le système d'information : o verrouille le compte ou le nœud pendant une période réglable dans le système; o verrouille le compte ou le nœud jusqu'à ce qu'un administrateur le déverrouille; o retarde, en fonction d'un délai réglable dans le système, la prochaine invitation à ouvrir une session dans le cas où le nombre maximum de tentatives infructueuses est dépassé. Cette mesure s'applique peu importe si la tentative d'ouverture de session est effectuée au moyen d'une connexion locale ou réseau.	✓	
AC-08	AVIS D'UTILISATION DU SYSTÈME	• Avant que l'accès au système soit accordé, le système d'information affiche un message ou un bandeau d'avis d'utilisation autorisée du système dans lequel figurent des avis de confidentialité et de sécurité conformément à la *Politique d'utilisation des réseaux électroniques* du SCT. • Le message ou le bandeau d'avis demeure à l'écran jusqu'à ce que l'utilisateur prenne des mesures explicites pour ouvrir une session ou accéder au système d'information. • Le système d'information, pour les systèmes accessibles au public : (i) affiche l'information sur l'utilisation du système, s'il y a lieu, avant de donner accès au système; (ii) affiche des références, le cas échéant, relatives à la surveillance, à l'enregistrement ou à la vérification qui sont conformes aux modalités de confidentialité de tels systèmes, qui interdisent généralement ces activités; (iii) inclut, dans l'avis donné aux utilisateurs publics du système d'information, une description des utilisations autorisées du système.	✓ ✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AC-09	AVIS D'OUVERTURE DE SESSION (ACCÈS) ANTÉRIEURE	• Le système d'information avise l'utilisateur, lorsqu'il ouvre une session (accède au système), de la date et de l'heure de la dernière ouverture de session (accès).	✓	
AC-09-01	AVIS D'OUVERTURE DE SESSION (ACCÈS) ANTÉRIEURE	• Le système d'information avise l'utilisateur : ○ lorsqu'il ouvre une session (accède au système), du nombre de tentatives infructueuses d'ouverture de session (accès) depuis la dernière ouverture de session (accès); ○ du nombre de tentatives infructueuses d'ouverture de session (accès) faites au cours d'une période réglable dans le système; ○ des modifications relatives à la sécurité apportées à son compte au cours d'une période réglable dans le système.		✓
AC-11	VERROUILLAGE DE SESSION	• Le système d'information empêche l'accès au système en verrouillant la session au terme d'une période d'inactivité (réglable dans le système) ou à la réception d'une demande de l'utilisateur. • Le système d'information garde la session verrouillée jusqu'à ce que l'utilisateur rétablisse l'accès en suivant les procédures d'identification et d'authentification établies.	✓ ✓	
AC-11-01	VERROUILLAGE DE SESSION	• À son activation dans un appareil doté d'un écran, le mécanisme de verrouillage de session du système d'information affiche un motif visible au public afin de cacher ce qui était auparavant visible.		✓
AC-14	ACTIVITÉS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION	• Le fournisseur de services détermine les activités précises que les utilisateurs peuvent accomplir dans le système d'information sans identification ni authentification. • Le fournisseur de services précise et justifie, dans le plan de sécurité des opérations du système d'information, les activités que les utilisateurs peuvent accomplir sans identification ni authentification.	✓ ✓	
AC-14-01	ACTIVITÉS PERMISES SANS IDENTIFICATION NI	• Le fournisseur de services autorise les activités qui peuvent être accomplies sans identification ni authentification seulement dans la mesure nécessaire pour réaliser la mission ou les objectifs		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	AUTHENTIFICATION	opérationnels.		
AC-16	CARACTÉRISTIQUES DE SÉCURITÉ	• Le système d'information permet et maintient l'association de caractéristiques de sécurité avec l'information stockée, en traitement et en cours de transmission.	✓	
AC-16-01	CARACTÉRISTIQUES DE SÉCURITÉ	• Le système d'information permet à des entités autorisées de modifier les caractéristiques de sécurité. • Le système d'information permet à des utilisateurs autorisés d'associer des caractéristiques de sécurité à l'information. • Le système d'information affiche, dans un format lisible par l'utilisateur, les caractéristiques de sécurité relatives à chaque sortie d'objet du système vers des appareils de sortie du système. L'opération vise à indiquer les directives spéciales de diffusion, de traitement ou de distribution à l'aide de conventions d'appellations standards lisibles par l'utilisateur.		✓ ✓ ✓
AC-17	ACCÈS À DISTANCE	• Le fournisseur de services : ○ met par écrit les méthodes autorisées d'accès à distance au système d'information; ○ applique des restrictions d'utilisation et des directives de mise en œuvre de chacune des méthodes d'accès à distance autorisées; ○ surveille le système d'information pour détecter les accès à distance non autorisés; ○ autorise l'accès à distance au système d'information avant la connexion; ○ applique les exigences relatives aux connexions à distance au système d'information; ○ veille à ce que tous les employés qui travaillent à l'extérieur des bureaux protègent les renseignements conformément aux exigences minimales précisées dans la *Norme opérationnelle sur la sécurité matérielle* du SCT.	✓	
AC-17-01	ACCÈS À DISTANCE	• Le fournisseur de services : ○ recourt à des mécanismes automatiques pour faciliter la		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		surveillance et le contrôle des méthodes d'accès à distance; ○ utilise la cryptographie pour préserver la confidentialité et l'intégrité des sessions qui se déroulent à distance. Le procédé cryptographique doit être conforme aux exigences de la mesure de contrôle SC-13; ○ autorise l'application de commandes et l'accès privilégiés à des renseignements liés à la sécurité par l'intermédiaire d'un accès à distance seulement dans le cas où il faut répondre à des besoins opérationnels urgents. De plus, il consigne la justification nécessaire à un tel accès dans le plan de sécurité du système d'information; ○ surveille le système d'information pour détecter les connexions à distance non autorisées et, le cas échéant, prend les mesures appropriées au moins une fois par année; ○ veille à ce que les utilisateurs protègent l'information sur les mécanismes d'accès à distance contre l'utilisation et la divulgation non autorisées; ○ veille à ce que les sessions distantes établies pour accéder aux fonctions de sécurité et aux renseignements liés à la sécurité fassent l'objet d'une vérification et de mesures de sécurité supplémentaires; ○ désactive les protocoles réseau jugés non sécuritaires dans le système d'information, sauf ceux utilisés dans les composants désignés explicitement comme des composants à l'appui d'exigences opérationnelles précises. • Le système d'information fait passer tous les accès à distance par un nombre limité de points de contrôle d'accès gérés. • L'accès à distance à des comptes privilégiés est établi à partir de consoles de gestion réservées, régies entièrement par les politiques de sécurité du système et utilisées exclusivement à cette fin (c'est-à-dire par exemple que l'accès Internet n'est pas autorisé).		✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AC-18	ACCÈS SANS FIL	• Le fournisseur de services : ○ établit les restrictions d'utilisation et les directives de mise en œuvre de l'accès sans fil; ○ surveille le système d'information pour détecter les accès sans fil non autorisés; ○ autorise l'accès sans fil au système d'information avant la connexion; ○ applique les exigences relatives aux connexions sans fil au système d'information.	✓	
AC-18-01	ACCÈS SANS FIL	• Le système d'information protège l'accès sans fil au moyen de dispositifs d'authentification et de cryptage. • Le fournisseur de services, au moins une fois par année : ○ fait le suivi des connexions sans fil non autorisées au système d'information, notamment en balayant le système pour déceler les points d'accès sans fil non autorisés, et prend le cas échéant les mesures appropriées; ○ interdit aux utilisateurs de configurer de façon indépendante les capacités de réseautage sans fil; ○ désactive les capacités de réseautage sans fil intégrées aux composants du système d'information, dans le cas où l'on ne prévoit pas utiliser celles-ci. La désactivation doit se faire avant la distribution et la mise en œuvre de ces composants.		✓ ✓
AC-19	CONTRÔLE D'ACCÈS POUR LES APPAREILS MOBILES	• Le fournisseur de services : ○ établit les restrictions d'utilisation et les directives de mise en service des appareils mobiles gérés par l'organisation; ○ autorise les connexions à ses systèmes d'information faites au moyen d'appareils mobiles qui respectent les restrictions d'utilisation et ses directives de mise en service du fournisseur de services; ○ surveille ses systèmes d'information pour détecter les connexions non autorisés faites au moyen d'appareils mobiles;	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ applique les exigences relatives aux connexions à ses systèmes d'information faites au moyen d'appareils mobiles; ○ désactive, dans ses systèmes d'information, la fonction permettant l'exécution automatique, non voulue par l'utilisateur, de codes dans les appareils mobiles; ○ fournit des appareils mobiles configurés spécialement aux personnes qui se rendent à des endroits qu'il considère comme présentant un risque considérable, conformément aux politiques et procédures du fournisseur de services; ○ applique des mesures préventives et d'inspection aux appareils mobiles qui reviennent d'endroits qu'il considère comme présentant un risque considérable, conformément aux politiques et procédures du fournisseur de services.		
AC-19-01	CONTRÔLE D'ACCÈS POUR LES APPAREILS MOBILES	• Le fournisseur de services : ○ limite l'utilisation de supports d'information inscriptibles amovibles dans les systèmes d'information visés; ○ interdit l'utilisation de supports d'information personnels amovibles dans les systèmes d'information visés; ○ interdit l'utilisation, dans les systèmes d'information visés, de supports d'information amovibles dont il est impossible d'identifier le propriétaire; ○ veille à ce que les utilisateurs éteignent les appareils sans fil disposant d'une fonction de transmission de la voix, ou qu'ils ferment le microphone lorsqu'ils assistent à des réunions où sont communiqués des renseignements Protégé B, Protégé C ou classifiés, conformément à la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* du SCT.		✓ ✓ ✓ ✓
AC-20	UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES	• S'appuyant sur les relations de confiance établies avec d'autres organisations possédant, exploitant ou entretenant des systèmes d'information externes, le fournisseur de services définit les modalités et conditions permettant à des personnes autorisées : ○ d'accéder au système d'information à partir de systèmes	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		d'information externes; ○ de traiter, de stocker ou de transmettre, à l'aide des systèmes d'information externes, des renseignements dont l'organisation a la garde.		
AC-20-01	UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES	• Le fournisseur de services permet aux personnes autorisées d'utiliser un système d'information externe pour accéder au système d'information ou pour traiter, stocker ou transmettre des renseignements dont l'organisation a la garde uniquement si l'une ou l'autre des conditions suivantes est remplie : (a) il peut s'assurer de la mise en œuvre des contrôles de sécurité requis dans le système externe, comme le précise sa politique et son plan sur la sécurité de l'information et son plan de sécurité; (b) il a approuvé la connexion du système d'information ou les ententes de traitement avec l'entité qui héberge le système d'information externe. • Le fournisseur de services limite l'utilisation des supports de stockage amovibles gérés par l'organisation aux personnes autorisées à utiliser les systèmes d'information externes.		✓ ✓
AC-21	COLLABORATION ET ÉCHANGE D'INFORMATION ENTRE UTILISATEURS	• Le fournisseur de services : ○ facilite l'échange d'information en permettant aux utilisateurs autorisés de déterminer si les autorisations d'accès attribuées à l'autre partie respectent les restrictions applicables en la matière; ○ s'appuie sur les mécanismes ou les procédures manuelles et sur les circonstances de l'échange d'information définis par l'organisation pour pour aider les utilisateurs à prendre des décisions à l'égard de l'échange d'information et de la collaboration.	✓	
AC-21-01	COLLABORATION ET ÉCHANGE D'INFORMATION ENTRE UTILISATEURS	• Le fournisseur de services assure, au moyen d'ententes écrites, la protection adéquate des renseignements de nature délicate échangés avec d'autres gouvernements et organisations.		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AC-22	CONTENU ACCESSIBLE AU PUBLIC	• Le fournisseur de services : ○ désigne les personnes autorisées à publier des renseignements dans un système d'information organisationnel accessible au public; ○ donne aux personnes autorisées une formation pour s'assurer qu'aucun renseignement confidentiel de nature délicate ne fait partie des renseignements accessibles au public; ○ examine, avant la publication dans un système d'information, le contenu que l'on propose de rendre accessible au public pour vérifier que celui-ci ne comporte aucun renseignement confidentiel de nature délicate; ○ examine, au moins une fois par année, le contenu déjà publié dans le système d'information accessible au public pour vérifier que celui-ci ne comporte aucun renseignement confidentiel de nature délicate; ○ retire du système d'information accessible au public tout renseignement confidentiel de nature délicate.	✓	

1.3 Vérification et responsabilisation (AU)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la vérification et de la responsabilisation et s'appliquant au service de débit pré-autorisé.

Tableau C-3 : Liste des exigences en matière de vérification et de responsabilisation

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AU-02	ÉVÉNEMENTS VÉRIFIABLES	• Le fournisseur de services établit, en fonction de la mission, des besoins opérationnels et de l'évaluation des risques, que le système d'information doit pouvoir vérifier tous les événements vérifiables. • Le fournisseur de services coordonne la fonction de vérification de sécurité avec les autres entités ayant besoin de renseignements liés à la vérification pour améliorer le soutien mutuel et pour contribuer à la sélection d'événements vérifiables. • Le fournisseur de services doit expliquer pourquoi il considère la liste d'événements vérifiables comme adéquate pour appuyer les enquêtes consécutives à des incidents relatifs à la sécurité. • Le fournisseur de services établit, en fonction des menaces actuelles pour l'information et de l'évaluation continue des risques, que les événements seront vérifiés dans le système d'information ainsi que la fréquence de vérification (ou les situations requérant une vérification) pour chacun des événements désignés.	✓ ✓ ✓ ✓	
AU-02-01	ÉVÉNEMENTS VÉRIFIABLES	• Le fournisseur de services examine et met à jour la liste des événements vérifiables au moins une fois par année. • Le fournisseur de services inclut l'exécution des fonctions privilégiées à la liste des événements que le système d'information doit vérifier.		✓ ✓
AU-03	CONTENU DES DOSSIERS DE VÉRIFICATION	• Le système d'information doit générer des dossiers de vérification permettant, au minimum, d'établir le type	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		d'événement survenu, la date et l'heure, la nature de l'événement, l'endroit où il s'est produit, sa source, le résultat (succès ou échec) ainsi que l'identité de tout utilisateur ou sujet associé à l'événement.		
AU-03-01	CONTENU DES DOSSIERS DE VÉRIFICATION	• Dans les dossiers de vérification, le système d'information intègre des renseignements détaillés sur les vérifications effectuées, désignées par type, par emplacement ou par sujet.		✓
AU-04	CAPACITÉ DE STOCKAGE DES DOSSIERS DE VÉRIFICATION	• Le fournisseur de services prévoit une capacité de stockage des dossiers de vérification et configure la vérification de façon à réduire la probabilité que cette capacité soit dépassée.	✓	
AU-05	INTERVENTION EN CAS D'ANOMALIE DU PROCESSUS DE VÉRIFICATION	• En cas d'anomalie du processus de vérification, le système d'information avertit les représentants désignés du fournisseur de services. • Le système d'information prend alors des mesures supplémentaires : arrêt du système, écrasement des plus anciens dossiers de vérification, arrêt de la production de dossiers de vérification, etc.	✓ ✓	
AU-05-01	INTERVENTION EN CAS D'ANOMALIE DU PROCESSUS DE VÉRIFICATION	• Le système d'information génère un avertissement lorsque le volume des dossiers de vérification stockés atteint un certain pourcentage (réglable dans le système) de la capacité maximale.		✓
AU-06	EXAMEN ET ANALYSE DES VÉRIFICATIONS ET PRODUCTION DES RAPPORTS CONNEXES	• Le fournisseur de services examine et analyse, à intervalles réguliers, les dossiers de vérification du système d'information pour vérifier la présence d'indices d'activités inappropriées ou inhabituelles, et présente le rapport de ses constatations à ses représentants désignés. • Le fournisseur de services adapte le nombre de vérifications examinées, analysées et faisant l'objet d'un rapport dans le système d'information en cas de changements relatifs au risque pour les activités et les biens de fournisseurs de	✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		service, pour les personnes, pour d'autres organisations ou pour le Canada selon les renseignements concernant le respect des lois, les renseignements secrets ou d'autres sources de renseignements crédibles.		
AU-06-01	EXAMEN ET ANALYSE DES VÉRIFICATIONS ET PRODUCTION DES RAPPORTS CONNEXES	• Le système d'information intègre les processus d'examen et d'analyse des vérifications ainsi que de production des rapports connexes pour soutenir les processus qu'emploie le fournisseur de service pour enquêter et intervenir en cas d'activités suspectes. • Le fournisseur de services analyse et met en corrélation les dossiers de vérification tirés de divers répertoires pour acquérir une connaissance de la situation à l'échelle de l'organisation. • Le système d'information centralise les examens et les analyses de dossiers de vérification tirés de plusieurs composants du système. • Le fournisseur de services précise, dans la politique de vérification et de responsabilisation, les actions autorisées par processus, par rôle et/ou par utilisateur autorisé du système d'information.		✓ ✓ ✓ ✓
AU-07	RÉDUCTION DES VÉRIFICATIONS ET PRODUCTION DE RAPPORTS	• Le système d'information comprend une fonction de réduction des vérifications et de production de rapports.	✓	
AU-07-01	RÉDUCTION DES VÉRIFICATIONS ET PRODUCTION DE RAPPORTS	• Le système d'information comprend une fonction de traitement automatique des dossiers de vérification des événements d'intérêt, dont les critères sont réglables.		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AU-08	HORODATAGE	• Le système d'information utilise ses horloges internes pour consigner l'heure et la date des dossiers de vérification.	✓	
AU-08-01	HORODATAGE	• Le système d'information synchronise, au moins une fois par année, ses horloges internes avec celles d'une source faisant autorité.		✓
AU-09	PROTECTION DES RENSEIGNEMENTS DE VÉRIFICATION	Le système d'information protège les renseignements de vérification et les outils de vérification contre les accès non autorisés, les modifications et la suppression.	✓	
AU-09-01	PROTECTION DES RENSEIGNEMENTS DE VÉRIFICATION	• Le système d'information sauvegarde, à intervalles réguliers, les dossiers de vérification sur un système ou un support d'information autre que celui qu'il vérifie. • Le fournisseur de services : (a) autorise l'accès aux fonctions de gestion de la vérification uniquement à un sous-ensemble limité d'utilisateurs privilégiés; (b) limite aux comptes privilégiés les accès extérieurs aux dossiers de vérification et l'exécution des fonctions privilégiées.		✓ ✓
AU-10	NON-RÉPUDIATION	• Le système d'information interdit à toute personne de nier faussement d'avoir exécuté une action en particulier.	✓	
AU-10-01	NON-RÉPUDIATION	• Le système d'information associe l'identité du producteur d'information à l'information produite. • Le système d'information valide le lien entre l'identité du producteur d'information et l'information produite. • Le système d'information conserve les authentifiants et l'identité des personnes responsables de la révision et de la diffusion dans la chaîne de possession établie pour toute information révisée ou publiée.		✓ ✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		• Le système d'information valide le lien entre l'identité du réviseur et l'information au moment de la diffusion ou du transfert, avant de diffuser ou de transférer l'information d'un domaine de sécurité à un autre. • En ce qui concerne les signatures numériques, le fournisseur de services se sert de la cryptographie conformément aux exigences de la mesure de contrôle SC-13.		✓ ✓
AU-11	CONSERVATION DES DOSSIERS DE VÉRIFICATION	• Le fournisseur de services conserve les dossiers de vérification pendant une période conforme à la politique de conservation des dossiers afin d'appuyer les enquêtes consécutives aux incidents relatifs à la sécurité et de respecter les exigences réglementaires et du fournisseur en matière de conservation des renseignements.	✓	
AU-12	PRODUCTION DES DOSSIERS DE VÉRIFICATION	• Le système d'information comprend une fonction de production de dossiers de vérification pour la liste des événements vérifiables, définie au point AU-2, dans les composants du système. • Le système d'information permet au personnel désigné du fournisseur de services de sélectionner les événements vérifiables qui doivent être vérifiés par des composants particuliers du système. • Le système d'information produit des dossiers de vérification pour la liste d'événements vérifiables définie au point AU-2 et comportant le contenu défini au point AU-3.	✓ ✓ ✓	
AU-12-01	PRODUCTION DES DOSSIERS DE VÉRIFICATION	• Le système d'information compile les dossiers de vérification provenant de ses composants selon une piste de vérification (logique ou physique) à l'échelle du système et dépendante du temps, dans les limites du niveau de tolérance réglé dans le système pour les relations entre les marques d'horodatage de chaque dossier dans la piste de vérification. • Le système d'information produit une piste de vérification (logique ou physique) à l'échelle du système et composée des dossiers de vérification dans un format normalisé.		✓ ✓

1.4 Certification, accréditation et évaluation de sécurité (CA)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la certification, de l'accréditation et de l'évaluation de sécurité et s'appliquant au service de débit pré-autorisé.

Tableau C-4 : Liste des exigences en matière de certification, d'accréditation et d'évaluation de sécurité

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
CA-02	ÉVALUATIONS DE LA SÉCURITÉ	• Le fournisseur de services élabore un plan d'évaluation de la sécurité qui décrit la portée de l'évaluation, notamment : (a) les contrôles de sécurité et les améliorations apportées aux contrôles faisant l'objet d'une évaluation; (b) les procédures d'évaluation à utiliser pour déterminer l'efficacité des contrôles de sécurité; (c) l'environnement d'évaluation, l'équipe d'évaluation et les rôles et responsabilités en matière d'évaluation.	✓	
		• Le fournisseur de services évalue les contrôles de sécurité du système d'information pour déterminer dans quelle mesure les contrôles ont été mis en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités afin de répondre aux exigences liées aux contrôles de sécurité du système.	✓	
		• Le fournisseur de services produit un rapport d'évaluation de la sécurité qui présente les résultats de l'évaluation.	✓	
		• Le fournisseur de services transmet par écrit les résultats de l'évaluation des contrôles de sécurité au représentant autorisé ou à la personne désignée par ce dernier.	✓	
CA-02-01	ÉVALUATIONS DE LA SÉCURITÉ	• Dans le cadre de ses évaluations de la sécurité effectuées à intervalles réguliers, le fournisseur de services inclut au moins les éléments suivants : o des évaluations annoncées; o des évaluations inopinées; o un contrôle approfondi; o des essais d'utilisateur malveillant;		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ des essais de pénétration; ○ des exercices selon la méthode de l'« équipe rouge ».		
CA-03	CONNEXIONS AU SYSTÈME D'INFORMATION	• Le fournisseur de services autorise les connexions entre le système d'information et les systèmes d'information qui ne sont pas compris dans la sphère d'autorisation par l'intermédiaire d'ententes sur la sécurité des interconnexions. • Pour chaque connexion, le fournisseur de services consigne les caractéristiques des interfaces, les exigences liées aux contrôles de sécurité et la nature de l'information transmise. • Le fournisseur de services surveille en continu les connexions au système d'information afin de vérifier le respect des exigences liées aux contrôles de sécurité.	✓ ✓ ✓	
CA-05	PLAN D'ACTION ET JALONS	• Le fournisseur de services : ○ élabore un plan d'action et établit des jalons relativement au système d'information afin de consigner les mesures correctives prévues pour corriger les points faibles ou combler les lacunes décelées au cours de l'évaluation des contrôles de sécurité et pour réduire, voire éliminer les vulnérabilités du système; ○ met à jour, au moins une fois par année, le plan d'action et les jalons, en fonction des conclusions découlant des évaluations des contrôles de sécurité, des analyses des répercussions sur la sécurité et des activités de contrôle continu.	✓	
CA-06	AUTORISATION DE SÉCURITÉ	• Le fournisseur de services : ○ désigne un cadre supérieur ou un gestionnaire principal à titre de responsable des autorisations pour le système d'information; ○ veille à ce que le responsable autorise le traitement par le système d'information avant d'entreprendre	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		toute opération; ○ met à jour, au moins une fois par année, l'autorisation de sécurité.		
CA-07	CONTRÔLE CONTINU	• Le fournisseur de services prépare une stratégie de contrôle continu et met en œuvre un programme de contrôle continu qui : ○ comprend un processus de gestion de la configuration du système d'information et de ses composants; ○ précise les répercussions sur la sécurité des modifications du système d'information et de son environnement d'exploitation; ○ comprend des évaluations constantes des contrôles de sécurité, conformément à la stratégie adoptée; ○ prévoit, au moins une fois par année, la production de rapports sur l'état de la sécurité du système d'information destinés aux représentants du fournisseur de services.	✓	
CA-07-01	CONTRÔLE CONTINU	• Le fournisseur de services planifie, prévoit et exécute, au moins une fois par année : ○ des évaluations annoncées; ○ des évaluations inopinées; ○ un contrôle approfondi; ○ des essais d'utilisateur malveillant; ○ des essais de pénétration; ○ des exercices selon la méthode de l'« équipe rouge », de manière à respecter l'intégralité des procédures de réduction des vulnérabilités.		✓

1.5 Gestion de la configuration (CM)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la gestion de la configuration et s'appliquant au service de débit pré-autorisé.

Tableau C-5 : Liste des exigences en matière de gestion de la configuration

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
CM-02	CONFIGURATION DE BASE	• Le fournisseur de services élabore, consigne, tient à jour la configuration de base du système d'information et en assure le contrôle.	✓	
CM-02-01	CONFIGURATION DE BASE	• Le fournisseur de services examine et met à jour la configuration de base du système d'information : (a) au moins une fois par année; (b) au besoin, lorsque les circonstances le justifient (la justification étant consignée et approuvée officiellement); (c) dans le cadre des installations et des mises à niveau du système d'information. • Le fournisseur de services recourt à des mécanismes automatisés pour maintenir la configuration de base du système d'information à jour, complète, précise et rapidement utilisable. • Le fournisseur de services : (a) développe et assure la tenue des logiciels dont l'utilisation est autorisée dans le système d'information; (b) applique une politique de refus global (autorisation par exception) afin de déterminer les logiciels qu'il est permis d'utiliser dans le système d'information. • Le fournisseur de services tient à jour une configuration de base des environnements de développement et d'essai, qui est gérée séparément de la configuration de base de l'environnement opérationnel.		✓ ✓ ✓ ✓
CM-03	CONTRÔLE DE LA MODIFICATION DE LA	• Le fournisseur de services : o recourt à des mécanismes pour modifier la	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	CONFIGURATION	configuration de base du système d'information et déploie la configuration mise à jour dans l'ensemble du parc informatique; ○ détermine les types de modifications du système d'information qui sont contrôlées au moyen de la configuration; ○ approuve les modifications contrôlées au moyen de la configuration en tenant explicitement compte des analyses des répercussions sur la sécurité; ○ consigne les modifications du système contrôlées au moyen de la configuration; ○ conserve et examine les dossiers des modifications du système contrôlées au moyen de la configuration; ○ vérifie les activités liées aux modifications du système contrôlées au moyen de la configuration; ○ coordonne et supervise les activités de contrôle des modifications de la configuration par l'intermédiaire d'un élément de contrôle qui se réunit au moins une fois par année; ○ met à l'essai, valide et consigne les modifications du système d'information avant qu'elles soient effectuées dans le système opérationnel; ○ exige qu'un représentant du secteur de la sécurité de l'information soit membre de l'élément de contrôle de la modification de la configuration.		
CM-04	ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ	• Le fournisseur de services analyse les modifications du système d'information avant de les effectuer afin de déterminer les répercussions possibles sur la sécurité.	✓	
CM-04-01	ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ	• Le fournisseur de services analyse les nouveaux logiciels dans un environnement d'essai distinct avant leur installation dans un environnement opérationnel afin de déterminer les répercussions sur la sécurité attribuables aux défauts, aux points faibles, à l'incompatibilité ou à la malveillance		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		intentionnelle. • Après la modification du système d'information, le fournisseur de services vérifie les fonctions de sécurité pour s'assurer qu'elles ont été mises en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités par rapport aux exigences liées aux contrôles de sécurité du système.		✓
CM-05	RESTRICTIONS D'ACCÈS EN MATIÈRE DE MODIFICATIONS	• Le fournisseur de services définit, consigne, approuve et applique les restrictions d'accès physique et logique associées aux modifications du système d'information.	✓	
CM-05-01	RESTRICTIONS D'ACCÈS EN MATIÈRE DE MODIFICATIONS	• Le fournisseur de services : ○ recourt à des mécanismes automatisés pour appliquer les restrictions d'accès et soutenir la vérification des mesures d'application; ○ vérifie, au moins une fois par année, les modifications apportées au système d'information et, lorsque les circonstances le justifient, détermine si des modifications non autorisées ont été apportées; ○ limite les privilèges des développeurs et des intégrateurs du système d'information à la modification directe des composants matériels, des logiciels et des micrologiciels ainsi que du système d'information dans un environnement de production; ○ examine et réévalue, au moins une fois par année, les privilèges des développeurs et des intégrateurs du système d'information; ○ limite les privilèges à la modification des logiciels internes dans les bibliothèques de logiciels (y compris les programmes privilégiés). • Le système d'information applique automatiquement des mesures de protection et de prévention si les fonctions ou les mécanismes de sécurité sont modifiés de façon inappropriée.		✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
CM-06	PARAMÈTRES DE CONFIGURATION	• Le fournisseur de services : ○ établit et consigne les paramètres de configuration obligatoires des produits de technologie de l'information utilisés dans le système d'information en utilisant des listes de vérification de la configuration de sécurité qui reflètent le mode le plus restrictif, conformément aux exigences opérationnelles; ○ met en place les paramètres de configuration; ○ répertorie, consigne et approuve les exceptions relatives aux paramètres de configuration obligatoires des composants distincts du système d'information en fonction des besoins opérationnels explicites; ○ surveille et contrôle les modifications apportées aux paramètres de configuration conformément aux politiques et aux procédures organisationnelles.	✓	
CM-06-01	PARAMÈTRES DE CONFIGURATION	• Le fournisseur de services : ○ emploie des mécanismes automatisés pour gérer, appliquer et vérifier les paramètres de configuration, le tout de façon centralisée; ○ emploie des mécanismes automatisés pour intervenir en cas de modifications non autorisées des paramètres de configuration; ○ intègre la détection des modifications de la configuration non autorisées ayant des répercussions sur la sécurité à la capacité de réaction aux incidents afin de s'assurer que de tels événements, une fois détectés, font l'objet d'un suivi, d'une surveillance et de mesures correctives, et qu'ils sont consignés à des fins de documentation. • Le système d'information (y compris les modifications apportées à la configuration de base) est conforme aux directives en matière de configuration de la sécurité (c.-à-d. les listes de contrôle de la sécurité), avant d'être implanté dans un environnement de production.		✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
CM-07	FONCTIONNALITÉ RESTREINTE	• Le fournisseur de services configure le système d'information de manière à fournir seulement les fonctions essentielles. De plus, il interdit expressément ou restreint l'utilisation des fonctions, des ports, des protocoles et des services dont l'utilisation est interdite ou limitée.	✓	
CM-07-01	FONCTIONNALITÉ RESTREINTE	• Le fournisseur de services : ○ examine, au moins une fois par année, le système d'information pour déceler et éliminer les fonctions, les ports, les protocoles et les services qui ne sont pas nécessaires; ○ assure la conformité aux exigences d'enregistrement relatives aux fonctions, aux ports, aux protocoles ou aux services.		✓
CM-08	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	• Le fournisseur de services prépare, consigne et tient à jour un inventaire des composants du système d'information : ○ qui reflète fidèlement la composition du système au moment de l'inventaire; ○ qui est conforme aux limites d'autorisation du système d'information; ○ qui respecte le niveau de précision jugé nécessaire pour le suivi et la production des rapports; ○ qui comprend l'information jugée nécessaire pour exercer une responsabilité efficace à l'égard des biens; ○ qu'il met à la disposition de ses responsables désignés aux fins d'examen et de vérification.	✓	
CM-08-01	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	• Le fournisseur de services : ○ intègre la mise à jour de l'inventaire des composants du système d'information aux activités d'installation, de retrait et de mise à jour des composants du système d'information; ○ emploie des mécanismes automatisés pour aider à		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		tenir un inventaire des composants du système d'information à jour, complet, exact et facilement accessible; ○ emploie des mécanismes automatisés pour détecter l'ajout de composants ou de dispositifs non autorisés dans le système d'information; ○ désactive l'accès au réseau par ces composants et dispositifs ou avise ses représentants désignés; ○ inclut, dans les renseignements sur les responsabilités à l'égard des biens concernant les composants du système d'information, un moyen d'identification en indiquant : ▪ le nom, ▪ le poste, ▪ le rôle, des personnes responsables de la gestion de ces composants; ○ vérifie que tous les composants dans les limites d'autorisation du système d'information sont inventoriés comme faisant partie intégrante du système ou qu'ils sont reconnus par un autre système en tant que composants de ce dernier; ○ inclut, dans l'inventaire des composants du système d'information, toutes les configurations des composants évalués et toute dérogation approuvée aux configurations en vigueur à ce moment-là.		
CM-09	PLAN DE GESTION DES CONFIGURATIONS	• Le fournisseur de services rédige et met en œuvre un plan de gestion des configurations du système d'information qui : ○ décrit les rôles et responsabilités ainsi que les processus et procédures de gestion des configurations; ○ décrit les éléments de configuration du système d'information et indique à quel moment, dans le cycle de développement des systèmes, ces éléments sont intégrés à la gestion des configurations;	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ définit les modes d'identification des éléments de configuration à employer tout au long du cycle de développement des systèmes ainsi que le processus de gestion de la configuration de ces éléments.		

1.6 Planification d'urgence (CP)

Le tableau suivant répertorie les exigences en matière de sécurité des TI liées au domaine de la planification d'urgence et s'appliquant au service de débit pré-autorisé.

Tableau C-6 : Liste des exigences en matière de planification d'urgence

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
CP-02	PLAN D'URGENCE	• Le fournisseur de services : ○ élabore un plan d'urgence pour le système d'information : ▪ dans lequel il énumère les missions et fonctions opérationnelles essentielles et les exigences de planification d'urgence qui y sont associées; ▪ dans lequel il énonce des objectifs de rétablissement, des priorités de restauration, ainsi que des mesures; ▪ dans lequel il décrit les rôles et les responsabilités de chacune des personnes chargées d'intervenir en cas d'urgence, en indiquant les coordonnées de ces personnes; ▪ dans lequel il décrit les mesures qui seront prises pour assurer la continuité des missions et des fonctions opérationnelles essentielles malgré une perturbation, une compromission ou une panne du système d'information; ▪ dans lequel il décrit les mesures qui seront prises pour rétablir complètement le système d'information sans nuire aux mesures de sécurité prévues à l'origine et mises en œuvre; ▪ qui est examiné et approuvé par les représentants désignés du fournisseur de services; ○ distribue des copies du plan d'urgence aux membres du personnel d'urgence clés (identifiés par leur nom ou par leur rôle) et aux représentants clés de son entreprise.	✓	

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
CP-02-01	PLAN D'URGENCE	• Le fournisseur de services : ○ coordonne les activités de planification d'urgence avec les activités de gestion des incidents; ○ passe en revue le plan d'urgence du système d'information au moins une fois par année; ○ révise le plan d'urgence en tenant compte des changements survenus au sein de sa propre organisation, dans le système d'information ou dans le contexte opérationnel, ainsi que des problèmes éprouvés lors de la mise en œuvre, de l'exécution ou de la mise à l'essai du plan d'urgence; ○ communique les changements apportés au plan d'urgence aux membres du personnel d'urgence clés (identifiés par leur nom ou par leur rôle) et aux représentants clés de son entreprise; ○ coordonne l'élaboration du plan d'urgence avec les représentants de son entreprise responsables des plans connexes; ○ planifie les capacités en prévoyant une capacité suffisante pour assurer le traitement de l'information, les télécommunications et le soutien au milieu d'exploitation au cours des opérations d'urgence; ○ planifie la reprise, à la suite de l'activation du plan, des missions et fonctions opérationnelles essentielles dans les délais prévus (par le plan d'urgence); ○ planifie la reprise complète, à la suite de l'activation du plan, des missions et fonctions opérationnelles dans les délais prévus par le plan d'urgence; ○ prévoit la poursuite des missions et fonctions opérationnelles essentielles, avec peu de perte ou sans perte de continuité opérationnelle, et veille au maintien de cette continuité jusqu'à la restauration complète du système d'information aux principaux emplacements de traitement ou de stockage; ○ prévoit le transfert de toutes missions et fonctions opérationnelles essentielles, avec peu de perte ou		✓

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
		sans perte de la continuité opérationnelle, à d'autres emplacements de traitement et de stockage, et maintient cette continuité jusqu'à la restauration complète des principaux emplacements de traitement et de stockage.		
CP-03	FORMATION AUX MESURES D'URGENCE	• Le fournisseur de services forme les membres du personnel pour les préparer à assumer leurs rôles et responsabilités en cas d'urgence à l'égard du système d'information et tient des séances de formation d'appoint au moins une fois par année.	✓	
CP-03-01	FORMATION AUX MESURES D'URGENCE	• Le fournisseur de services intègre des simulations d'événements à la formation aux mesures urgence afin de mieux préparer le personnel à intervenir de manière efficace en situation de crise.		✓
CP-04	ESSAIS ET EXERCICES DE DÉPLOIEMENT DU PLAN D'URGENCE	• Au moins une fois par année, le fournisseur de services met à l'essai le plan d'urgence entourant le système d'information ou organise des exercices officiels pour déterminer si le plan est efficace et prêt à être exécuté. • Le fournisseur de services examine les résultats des essais et des exercices entourant le plan d'urgence et met en place des mesures correctives.	✓ ✓	
CP-04-01	ESSAIS ET EXERCICES DE DÉPLOIEMENT DU PLAN D'URGENCE	• Le fournisseur de services coordonne la mise à l'essai du plan d'urgence ou les exercices avec les représentants de son entreprise responsables des plans connexes. • Le fournisseur de services met à l'essai le plan d'urgence ou organise des exercices à l'emplacement de traitement de remplacement afin de familiariser le personnel chargé des mesures d'urgence avec l'installation et les ressources disponibles, et d'évaluer la capacité de cet emplacement à prendre en charge les opérations d'urgence.		✓ ✓
CP-06	EMPLACEMENT DE STOCKAGE DE	• Le fournisseur de services établit un emplacement de stockage de remplacement et conclut les accords nécessaires	✓	

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
	REMPLACEMENT	pour permettre le stockage et la récupération des données de sauvegarde du système d'information. • Le fournisseur de services désigne un emplacement de stockage de remplacement distinct de l'emplacement principal afin que ces deux emplacements ne soient pas exposés aux mêmes dangers.	✓	
CP-07	EMPLACEMENT DE TRAITEMENT DE REMPLACEMENT	• Le fournisseur de services établit un emplacement de traitement de remplacement et conclut les accords nécessaires pour permettre la reprise des activités du système d'information pour les missions et fonctions opérationnelles essentielles dans les délais correspondant aux objectifs fixés en matière de temps de récupération, lorsque les capacités de traitement principales ne sont pas disponibles. • Le fournisseur de services désigne un emplacement de traitement de remplacement distinct de l'emplacement principal afin que ces deux emplacements ne soient pas exposés aux mêmes dangers.	✓ ✓	
CP-07-01	EMPLACEMENT DE TRAITEMENT DE REMPLACEMENT	• Le fournisseur de services s'assure que l'emplacement de traitement de remplacement est doté de mesures de sécurité de l'information équivalentes à celles de l'emplacement principal.		✓
CP-08	SERVICES DE TÉLÉCOMMUNICATIONS	• Le fournisseur de services établit des services de télécommunications de remplacement et conclut les accords nécessaires pour permettre la reprise des activités du système d'information pour les missions et fonctions opérationnelles essentielles dans les délais prévus (par le plan d'urgence) lorsque les capacités de télécommunications principales ne sont pas disponibles.	✓	
CP-08-01	SERVICES DE TÉLÉCOMMUNICATIONS	• Le fournisseur de services : (a) conclut des ententes de services de télécommunications		✓

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
		principaux et de remplacement et veille à ce que ces ententes contiennent des dispositions liées à la priorité de services, conformément aux exigences de disponibilité; (b) exige la priorité de service à l'égard de tous les services de télécommunications utilisés pour la sûreté et les préparatifs d'urgence à l'échelle nationale au cas où les services de télécommunications principaux et de remplacement proviendraient d'un fournisseur unique. • Le fournisseur de services se procure des services de télécommunications de remplacement de manière à diminuer la probabilité d'être soumis à un point de défaillance unique des principaux services de télécommunications. • Le fournisseur de services conclut des ententes avec d'autres fournisseurs de services de télécommunications distincts des fournisseurs de services principaux afin que ces services ne soient pas exposés aux mêmes dangers.		✓ ✓
CP-09	SAUVEGARDE DU SYSTÈME D'INFORMATION	• Le fournisseur de services réalise des sauvegardes de l'information de niveau utilisateur contenue dans le système d'information à une fréquence respectant les objectifs en matière de délai de récupération et de point de récupération. • Le fournisseur de services réalise des sauvegardes de l'information de niveau système contenue dans le système d'information à une fréquence respectant les objectifs en matière de délai de récupération et de point de récupération. • Le fournisseur de services réalise des sauvegardes des documents du système d'information, dont les documents ayant trait à la sécurité, à une fréquence respectant les objectifs en matière de délai de récupération et de point de récupération. • Le fournisseur de services protège la confidentialité et l'intégrité des informations sauvegardées à l'emplacement de stockage conformément à la *Norme opérationnelle sur la sécurité matérielle* du SCT. • Le fournisseur de services fixe les périodes de conservation	✓ ✓ ✓ ✓ ✓	

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
		pour les renseignements opérationnels essentiels et les sauvegardes archivées. • Le fournisseur de services met à l'essai les données de sauvegarde pour vérifier la fiabilité des supports et l'intégrité des données au moins une fois par année.	✓	
CP-09-01	SAUVEGARDE DU SYSTÈME D'INFORMATION	• Le fournisseur de services utilise un échantillon de données de sauvegarde pour réaliser la restauration de certaines fonctions choisies du système d'information dans le cadre de l'essai du plan d'urgence. • Le fournisseur de services stocke des copies de sauvegarde du système d'exploitation et autres logiciels essentiels du système d'information, ainsi que des copies de l'inventaire du système d'information (y compris le matériel, les logiciels et les micrologiciels) dans une installation distincte ou dans un conteneur ignifuge, placé à un endroit distinct du système opérationnel. • Le fournisseur de services transfère les informations de sauvegarde du système d'information dans l'emplacement de stockage de remplacement selon la périodicité et les taux de transfert établis conformément aux objectifs en matière de délai de récupération et de point de récupération.		✓ ✓ ✓
CP-10	RÉCUPÉRATION ET RECONSTITUTION DU SYSTÈME D'INFORMATION	• Le fournisseur de services prévoit la récupération et la reconstitution du système d'information à un état précédent connu après une interruption, une compromission ou une panne.	✓	
CP-10-01	RÉCUPÉRATION ET RECONSTITUTION DU SYSTÈME D'INFORMATION	• Le système d'information exécute la récupération des transactions en ce qui concerne les systèmes fondés sur les transactions. • Le fournisseur de services offre la possibilité de restituer l'image des composants du système d'information dans les délais de restauration établis à partir d'images-disques dont la configuration est contrôlée et dont l'intégrité est protégée, de		✓ ✓

Point nº	Titre de l'exigence	Description	Référence	Supplémentaire
		manière à ramener les composants à un point de restauration sûr et opérationnel. • Le fournisseur de services protège le matériel, les micrologiciels et les logiciels de sauvegarde et de restauration.		✓

1.7 Identification et authentification (IA)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de l'identification et de l'authentification et s'appliquant au service de débit pré-autorisé.

Tableau C-7 : Liste des exigences en matière d'identification et d'authentification

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
IA-02	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DU FOURNISSEUR DE SERVICES)	• Le système d'information identifie et authentifie de manière unique les utilisateurs du fournisseur de services (ou les processus agissant au nom de ces derniers).	✓	
IA-02-01	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DU FOURNISSEUR DE SERVICES)	• Le système d'information utilise des mécanismes d'authentification résistants aux attaques par réinsertion pour l'accès à des comptes privilégiés et non privilégiés à partir du réseau. • Le système d'information utilise l'authentification multifactorielle pour l'accès à distance à des comptes privilégiés.		✓ ✓
IA-03	IDENTIFICATION ET AUTHENTIFICATION DES APPAREILS	• Le système d'information identifie et authentifie de manière unique tous les appareils avant d'établir une connexion.	✓	
IA-03-01	IDENTIFICATION ET AUTHENTIFICATION DES APPAREILS	• Le système d'information authentifie les appareils avant d'établir des connexions réseau à distance et sans fil en utilisant l'authentification bidirectionnelle entre les appareils basée sur la cryptographie. • En ce qui concerne l'attribution d'adresses dynamiques, le fournisseur de services normalise les données des baux DHCP et le temps attribué aux appareils, puis vérifie les données des baux lorsqu'elles sont attribuées à un appareil.		✓ ✓
IA-04	GESTION DES	• Le fournisseur de services gère les identifiants du	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	IDENTIFIANTS	système d'information pour les utilisateurs et les appareils en : ○ recevant d'un représentant désigné du fournisseur de services l'autorisation d'attribuer un identifiant à un utilisateur ou à un appareil; ○ sélectionnant un identifiant qui identifie de manière unique un individu ou un appareil; ○ attribuant l'identifiant de l'utilisateur à la partie visée ou l'identifiant de l'appareil à l'appareil visé; ○ empêchant la réutilisation des identifiants d'utilisateurs ou d'appareils pendant une période prédéfinie (configurable au moyen du système); ○ désactivant l'identifiant de l'utilisateur après une période d'inactivité donnée (paramètre configurable au moyen du système).		
IA-04-01	GESTION DES IDENTIFIANTS	• Le fournisseur de services : ○ interdit l'utilisation d'identifiants de comptes du système d'information comme identifiants publics pour les comptes d'utilisateurs de courrier électronique (c.-à-d. la partie « identifiant » de l'adresse de courrier électronique); ○ exige que l'enregistrement pour recevoir un code d'utilisateur et un mot de passe exige l'autorisation d'un superviseur, et qu'il se déroule en présence d'un responsable désigné pour l'enregistrement; ○ exige qu'une combinaison de différentes formes de certification de l'identification individuelle, comme une preuve documentaire ou une combinaison de documents et d'éléments biométriques, soit présentée au responsable de l'enregistrement; ○ gère les identifiants des utilisateurs en		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		identifiant ces derniers de manière unique.		
IA-05	GESTION DES AUTHENTIFICATEURS	• Le fournisseur de services gère les authentificateurs du système d'information pour les utilisateurs et les appareils en : ○ vérifiant, dans le cadre de la distribution d'authentificateurs initiale, l'identité de la personne ou de l'appareil qui reçoit l'authentificateur; ○ établissant le contenu initial des authentificateurs établis par le fournisseur de services; ○ veillant à ce que les authentificateurs soient dotés de mécanismes suffisamment résistants pour leur utilisation prévue; ○ établissant et en mettant en place des procédures administratives pour la distribution initiale des authentificateurs, pour la perte ou la compromission des authentificateurs, ainsi que pour la révocation des authentificateurs; ○ modifiant le contenu par défaut des authentificateurs lors de l'installation du système d'information; ○ établissant des restrictions quant à la durée de vie minimale et maximale, ainsi que les conditions de réutilisation des authentificateurs, s'il y a lieu; ○ modifiant ou en rafraîchissant la périodicité des authentificateurs pour chaque type d'authentificateur (une valeur configurable au moyen du système); ○ protégeant le contenu des authentificateurs de toute divulgation ou modification non autorisée; ○ exigeant des utilisateurs qu'ils prennent des mesures particulières pour protéger les authentificateurs et en exigeant que les	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		appareils mettent ces mesures en œuvre.		
IA-05-01	GESTION DES AUTHENTIFICATEURS	• Le système d'information, pour l'authentification par mot de passe : a) exige des mots de passe ayant une complexité minimale en ce qui a trait à la sensibilité à la casse, au nombre de caractères, à la combinaison de majuscules, de minuscules, de chiffres et de caractères spéciaux, y compris les exigences minimales pour chaque type de mot de passe; b) exige la modification d'au moins un certain nombre de caractères lors du changement de mot de passe; c) chiffre les mots de passe lors de leur stockage et de leur transmission; d) applique des restrictions quant à la durée de vie minimale et maximale des mots de passe; e) empêche la réutilisation des mots de passe pendant un certain nombre de générations. • Le système d'information, pour l'authentification par mot de passe : a) valide les certificats en constituant un chemin de certification vers une ancre de confiance reconnue; b) accorde un accès autorisé à la clé privée correspondante; c) met l'identité authentifiée en correspondance avec le compte d'utilisateur. • Le fournisseur de services : ○ exige que le processus d'inscription permettant de recevoir des types d'authentificateurs ou des authentificateurs précis soit réalisé en personne devant un responsable désigné de l'enregistrement, avec l'autorisation d'un représentant désigné par le fournisseur de services (p. ex. un superviseur); ○ protège les authentificateurs en fonction de la sensibilité et du caractère essentiel de		✓ ✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		l'information et du système d'information visé par la demande d'accès; ○ s'assure que les authentificateurs statiques non chiffrés ne sont pas intégrés dans des applications ou des scripts d'accès, ou encore stockés dans les touches de fonction; ○ prend des mesures pour gérer le risque de compromission découlant du fait que des personnes disposent de comptes sur plusieurs systèmes d'information.		
IA-06	AFFICHAGE DES RENSEIGNEMENTS D'AUTHENTIFICATION	• Le système d'information masque la rétroaction des renseignements d'authentification au cours du processus d'authentification pour protéger ces renseignements contre toute exploitation ou utilisation possible par des personnes non autorisées.	✓	
IA-07	AUTHENTIFICATION DU MODULE DE CHIFFREMENT	• Le système d'information utilise des mécanismes pour l'authentification auprès d'un module de chiffrement qui répond aux exigences édictées par les directives du Centre de la sécurité des télécommunications Canada (CSTC) applicables à ce type d'authentification.	✓	
IA-08	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS SANS LIEN AVEC LE FOURNISSEUR DE SERVICES)	• Le système d'information identifie et authentifie de manière unique les utilisateurs ne faisant pas partie de l'entité du fournisseur de services (ou les processus agissant au nom de ces derniers).	✓	

1.8 Réaction aux incidents (IR)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la réaction aux incidents et s'appliquant au service de débit pré-autorisé.

Tableau C-8 : Liste des exigences en matière de réaction aux incidents

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
IR-02	FORMATION EN MATIÈRE DE RÉACTION AUX INCIDENTS	• Le fournisseur de services forme les membres du personnel pour qu'ils connaissent leurs rôles et responsabilités en matière de réaction aux incidents en ce qui concerne le système d'information. • Le fournisseur de services tient des séances de formation d'appoint au moins une fois par année.	✓ ✓	
IR-02-01	FORMATION EN MATIÈRE DE RÉACTION AUX INCIDENTS	• Le fournisseur de services intègre des simulations d'événements à la formation liée à la réaction aux incidents afin de mieux préparer le personnel à intervenir de manière efficace en situation de crise.		✓
IR-03	ESSAIS ET EXERCICES DE RÉACTION AUX INCIDENTS	• Le fournisseur de services réalise des essais ou des exercices au moins une fois par année pour vérifier la capacité de réaction aux incidents entourant le système d'information, de manière à pouvoir évaluer l'efficacité de la réaction aux incidents et à en consigner les résultats.	✓	
IR-04	TRAITEMENT DES INCIDENTS	• Le fournisseur de services met en place une capacité de traitement des incidents qui comprend la préparation, la détection et l'analyse, le confinement, l'éradication et la récupération. • Le fournisseur de services coordonne les activités de traitement des incidents avec les activités de planification d'urgence. • Le fournisseur de services intègre les leçons apprises des activités de traitement des incidents en cours à des	✓ ✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		procédures de réaction aux incidents, ainsi qu'à des formations, essais et exercices, puis met en œuvre les changements qui s'imposent à la lumière de ces leçons.		
IR-04-01	TRAITEMENT DES INCIDENTS	• Le fournisseur de services établit des catégories d'incidents et définit les mesures à prendre pour assurer la continuité des missions et des fonctions opérationnelles de son entreprise. • Le fournisseur de services établit une corrélation entre les données sur les incidents et les réactions à chaque incident afin d'avoir une perspective panorganisationnelle de la sensibilisation et de la réaction aux incidents.		✓ ✓
IR-05	SUIVI DES INCIDENTS	Le fournisseur de services fait le suivi des incidents de sécurité du système d'information et les met par écrit.	✓	
IR-06	SIGNALEMENT DES INCIDENTS	• Le fournisseur de services demande au personnel de signaler tout incident de sécurité présumé à sa capacité de réaction aux incidents dans les TROIS (3) mois suivant l'incident. • Le fournisseur de services présente les renseignements d'incidents de sécurité aux autorités désignées. • Le fournisseur de services présente à ses représentants appropriés un rapport sur les faiblesses, les lacunes ou les vulnérabilités du système d'information associées aux incidents de sécurité signalés.	✓ ✓ ✓	
IR-07	SOUTIEN À LA RÉACTION AUX INCIDENTS	Le fournisseur de services intègre à sa capacité de réaction aux incidents une ressource de soutien qui donne des conseils et du soutien aux utilisateurs du système d'information en ce qui a trait au traitement et au signalement des incidents de sécurité.	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
IR-08	PLAN D'INTERVENTION EN CAS D'INCIDENT	• Le fournisseur de services élabore un plan d'intervention en cas d'incident qui : (a) constitue sa feuille de route pour la mise en œuvre de sa capacité de réaction aux incidents; (b) décrit la structure et l'organisation de la capacité de réaction aux incidents; (c) fournit une approche d'ensemble concernant la façon dont la capacité de réaction aux incidents s'intègre dans l'organisation en général; (d) satisfait aux exigences uniques du fournisseur de services, lesquelles se rapportent à la mission, à la taille, à la structure et aux fonctions; (e) définit les incidents à signaler; (f) permet de mesurer la capacité de réaction aux incidents du fournisseur de services; (g) définit les ressources et le soutien de la gestion requis pour maintenir et faire évoluer de façon efficace la capacité de réaction aux incidents; (h) est examiné et approuvé par les représentants désignés du fournisseur de services. • Le fournisseur de services : ○ distribue des exemplaires du plan d'intervention en cas d'incident aux membres du personnel (désignés par nom ou par fonction) et aux éléments chargés d'intervenir en cas d'incident; ○ passe en revue le plan d'intervention en cas d'incident au moins une fois par année; ○ révise le plan d'intervention en cas d'incident pour l'adapter aux changements du système ou de son entreprise, ou pour régler les problèmes éprouvés pendant la mise en œuvre, l'exécution ou la mise à l'essai du plan; ○ communique les changements apportés au plan d'intervention en cas d'incident aux membres du personnel (identifiés par leur nom ou par leur	✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		rôle) et aux éléments de son entreprise chargés d'intervenir en cas d'incident.		

1.9 Maintenance du système (MA)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à la maintenance du système et s'appliquant au service de débit pré-autorisé.

Tableau C-9 : Liste des exigences en matière de maintenance du système

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
MA-02	MAINTENANCE DIRIGÉE	• Le fournisseur de services : ○ planifie, exécute, et consigne la maintenance et les réparations des composants du système d'information conformément à ses propres exigences ou spécifications, ou à celles du fabricant, et examine les dossiers de maintenance; ○ dirige toutes les activités de maintenance, qu'elles soient exécutées sur les lieux ou à distance, et que l'équipement soit entretenu sur les lieux ou dans un autre emplacement; ○ doit demander l'autorisation expresse d'un représentant désigné pour sortir certains composants du système d'information ou le système lui-même des installations de fournisseur de services aux fins de maintenance ou de réparations hors site; ○ nettoie l'équipement afin d'effacer tous les renseignements des supports d'information qui y sont associés avant de le sortir de ses installations aux fins de maintenance ou de réparations hors site; ○ vérifie tous les contrôles de sécurité susceptibles d'être perturbés pour s'assurer qu'ils fonctionnent toujours correctement à la suite des activités de maintenance ou de réparation.	✓	
MA-02-01	MAINTENANCE DIRIGÉE	• Le fournisseur de services conserve des dossiers de maintenance du système d'information comportant notamment : a) la date et l'heure de la maintenance;		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		b) le nom de la personne qui a exécuté la maintenance; d) le nom de l'accompagnateur, le cas échéant; e) une description de l'activité de maintenance exécutée; f) une liste de l'équipement retiré ou remplacé (y compris les numéros d'identification, le cas échéant).		
MA-03	OUTILS DE MAINTENANCE	• Le fournisseur de services approuve, contrôle et entretient de façon continue les outils de maintenance du système d'information et en surveille l'utilisation.	✓	
MA-03-01	OUTILS DE MAINTENANCE	• Le fournisseur de services vérifie que tous les supports d'information contenant des programmes de diagnostic et de mise à l'essai ne comportent aucun programme malveillant avant d'autoriser leur utilisation dans le système d'information.		✓
MA-04	MAINTENANCE EXTERNE	• Le fournisseur de services autorise, surveille et contrôle les activités de maintenance et de diagnostic externes. ✓ • Le fournisseur de services permet l'utilisation d'outils de maintenance et de diagnostic externes uniquement s'ils sont conformes à sa politique et consignés dans le plan de sécurité du système d'information. ✓ • Le fournisseur de services utilise des techniques fiables d'identification et d'authentification dans le cadre des séances de maintenance et de diagnostic externes. ✓ • Le fournisseur de services conserve des dossiers sur les activités de maintenance et de diagnostic externes. ✓		
MA-04-01	MAINTENANCE EXTERNE	• Le fournisseur de services surveille les séances de maintenance et de diagnostic externes et le personnel désigné du fournisseur de services examine les dossiers de maintenance de ces séances. ✓ • Le fournisseur de services consigne, dans le plan de sécurité du système d'information, l'installation et l'utilisation de connexions externes aux fins de ✓		

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		maintenance et de diagnostic. • Le fournisseur de services : a) exige que les services de maintenance et de diagnostic externes soient exécutés depuis un système d'information où le niveau de sécurité mis en œuvre est au moins aussi élevé que celui du système faisant l'objet de la maintenance; b) retire le composant du système d'information devant faire l'objet de la maintenance et, avant l'exécution des services de maintenance et de diagnostic externes, nettoie le composant (pour effacer tout renseignement appartenant au fournisseur de services) avant de le sortir de ses installations. Une fois les services exécutés, il inspecte le composant et le nettoie à nouveau (pour supprimer tout logiciel malveillant ou tout élément implanté clandestinement) avant de le réinstaller dans le système d'information. • Le fournisseur de services protège les séances de maintenance externes en utilisant un authentificateur fiable, étroitement lié à l'utilisateur, et en isolant ces séances des autres séances du réseau dans le système d'information par l'un des moyens suivants : a) en utilisant des voies de communication séparées physiquement; b) en utilisant des voies de communication dont la séparation logique est fondée sur un chiffrement conforme aux exigences de la mesure de contrôle SC-13. • Le fournisseur de services exige que : a) le personnel de maintenance fournisse un avis lorsqu'une maintenance externe est prévue (indication de la date et de l'heure); b) l'un de ses représentants désignés qui connaît bien la sécurité de l'information et le système d'information approuve la maintenance externe.		✓ ✓ ✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		• Le fournisseur de services utilise des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications liées aux activités de maintenance et de diagnostic externes.		✓
MA-05	PERSONNEL DE MAINTENANCE	• Le fournisseur de services : ○ établit un processus d'autorisation du personnel de maintenance et conserve une liste à jour du personnel et des organismes de maintenance autorisés; ○ vérifie que le personnel qui procède à la maintenance du système d'information dispose des autorisations d'accès requises, ou désigne des membres de son personnel disposant des autorisations d'accès requises et des compétences techniques jugées nécessaires pour superviser la maintenance du système d'information si le personnel de maintenance ne dispose pas des autorisations d'accès requises.	✓	
MA-05-01	PERSONNEL DE MAINTENANCE	• Le fournisseur de services met en place des procédures relatives à l'utilisation de personnel de maintenance qui ne dispose pas d'une attestation de sécurité appropriée ou de la citoyenneté canadienne, comportant notamment les exigences suivantes : a) le personnel de maintenance ne disposant pas d'une autorisation d'accès, d'une attestation de sécurité ou d'une approbation d'accès officielle sera accompagné et supervisé par des membres du personnel du fournisseur de services dûment attestés, disposant d'une autorisation d'accès appropriée et qualifiés sur le plan technique pendant l'exécution des activités de maintenance et de diagnostic du système d'information; b) avant le début des activités de maintenance ou de diagnostic exécutées par le personnel ne disposant pas		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		d'une autorisation d'accès, d'une attestation de sécurité ou d'une approbation d'accès officielle, tous les composants de stockage d'information non rémanents du système d'information doivent être nettoyés et tous les supports d'information rémanents doivent être retirés ou débranchés physiquement du système et protégés; c) s'il s'avère qu'un composant du système d'information n'est pas nettoyable, les procédures énoncées dans le plan de sécurité du système sont appliquées.		
MA-06	MAINTENANCE EN TEMPS OPPORTUN	• Le fournisseur de services obtient du soutien de maintenance ou des pièces de rechange pour des composants du système d'information essentiels à la sécurité, ou encore des composants fondamentaux liés à la technologie de l'information à l'intérieur de la période (précisée dans le plan de continuité) suivant la défaillance.	✓	

1.10 Protection des supports d'information (MP)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à la protection des supports d'information et s'appliquant au service de débit pré-autorisé.

Tableau C-10 : Liste des exigences en matière d'intégrité du système et de l'information

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
MP-02	ACCÈS AUX SUPPORTS D'INFORMATION	• Le fournisseur de services restreint l'accès aux supports numériques et non numériques aux personnes autorisées au moyen de mesures de sécurité.	✓	
MP-02-01	ACCÈS AUX SUPPORTS D'INFORMATION	• Le fournisseur de services utilise des mécanismes automatisés pour restreindre l'accès aux zones de stockage des supports d'information et pour détecter les tentatives d'accès et les accès accordés. • Le système d'information utilise des mécanismes cryptographiques pour protéger et limiter l'accès à l'information stockée dans des supports numériques portatifs.		✓ ✓
MP-03	MARQUAGE DES SUPPORTS D'INFORMATION	• Conformément à ses politiques et procédures, le fournisseur de services marque les supports amovibles et les données de sortie du système d'information en indiquant les restrictions de diffusion, les oppositions et les marquages de sécurité applicables (le cas échéant) des renseignements. • Le fournisseur de services exempte les supports d'information amovibles du marquage tant que les supports exemptés demeurent dans les zones contrôlées.	✓ ✓	
MP-04	ENTREPOSAGE DES SUPPORTS D'INFORMATION	• Le fournisseur de services contrôle et entrepose de manière sécuritaire les supports numériques et non numériques dans les zones contrôlées, conformément aux exigences du *Guide d'équipement de sécurité* (G1-001) de la GRC. • Le fournisseur de services protège physiquement et entrepose de manière sécuritaire les supports du système	✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		comportant des renseignements protégés et classifiés en attente de destruction (sur les lieux ou hors site) en utilisant de l'équipement, des techniques et des procédures approuvés.		
MP-04-01	ENTREPOSAGE DES SUPPORTS D'INFORMATION	• Le fournisseur de services utilise des mécanismes cryptographiques pour protéger les renseignements entreposés.		✓
MP-05	TRANSPORT DES SUPPORTS D'INFORMATION	• Le fournisseur de services protège et contrôle les supports numériques et non numériques durant leur transport hors des zones contrôlées en utilisant des mesures de sécurité conformément à la *Norme opérationnelle sur la sécurité matérielle* du SCT et aux *Normes pour le transport ou la transmission de renseignements et de biens de nature délicate* (G1-009) de la GRC. • Le fournisseur de services demeure responsable des supports d'information du système pendant leur transport hors des zones contrôlées. • Le fournisseur de services limite les activités liées au transport des supports d'information au personnel autorisé.	✓ ✓ ✓	
MP-05-01	TRANSPORT DES SUPPORTS D'INFORMATION	• Le fournisseur de services consigne les activités liées au transport des supports d'information du système. • Le fournisseur de services utilise des mécanismes cryptographiques conformes aux exigences de la mesure de contrôle SC 13 pour protéger la confidentialité et l'intégrité des renseignements stockés dans les supports numériques pendant le transport hors des zones contrôlées.		✓ ✓
MP-06	NETTOYAGE DES SUPPORTS	• Le fournisseur de services nettoie les supports du système d'information, numériques et non numériques, avant leur élimination, leur retrait de son contrôle ou leur retrait en vue de leur réutilisation.	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		• Le fournisseur de services emploie des mécanismes de nettoyage dont la puissance et l'intégrité correspondent au classement ou au degré de confidentialité de l'information.	✓	
MP-06-01	NETTOYAGE DES SUPPORTS	• Le fournisseur de services suit, consigne et vérifie les activités de nettoyage et d'élimination des supports. • Le fournisseur de services contrôle le matériel et les procédures de nettoyage au moins une fois par année pour vérifier leur bon fonctionnement. • Le fournisseur de services nettoie les supports du système d'information qui contiennent des renseignements confidentiels conformément aux politiques, normes et procédures applicables du gouvernement du Canada. • Le fournisseur de services détruit les supports du système d'information qui ne peuvent être nettoyés.		✓ ✓ ✓ ✓

1.11 Domaine physique et environnemental (PE)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine physique et environnemental et s'appliquant au service de débit pré-autorisé.

Tableau C-11 : Liste des exigences relatives au domaine physique et environnemental

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
PE-02	AUTORISATION D'ACCÈS PHYSIQUE	• Le fournisseur de services dresse et actualise la liste du personnel autorisé à accéder à l'installation où se trouve le système d'information (sauf pour les zones de l'installation officiellement accessibles au public). • Le fournisseur de services fournit des justificatifs d'autorisation. • Le fournisseur de services examine et approuve la liste d'accès et les justificatifs d'autorisation au moins une fois par année, et il retire de la liste d'accès les membres du personnel qui n'ont plus besoin d'un accès.	✓ ✓ ✓	
PE-02-01	AUTORISATION D'ACCÈS PHYSIQUE	• Le fournisseur de services autorise l'accès physique à l'installation où se trouve le système d'information en fonction du poste ou du rôle occupé. • Le fournisseur de services remet une carte d'identification à tous les membres du personnel, laquelle doit au moins comporter le nom du fournisseur de services, le nom et la photo du titulaire, un numéro de carte unique et une date d'expiration.		✓ ✓
PE-03	CONTRÔLE DE L'ACCÈS PHYSIQUE	• Le fournisseur de services contrôle l'accès aux zones officiellement accessibles au public en fonction de son évaluation du risque. • Le fournisseur de services sécurise les clés, les combinaisons et les autres dispositifs d'accès physique. • Le fournisseur de services dresse la liste des dispositifs	✓ ✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		d'accès physiques au moins une fois par année. • Le fournisseur de services change les combinaisons et les clés au moins une fois par année, de même que lorsqu'une clé est perdue, une combinaison compromise ou des personnes mutées ou licenciées. • Le fournisseur de services gère les autorisations d'accès physique au système d'information indépendamment des contrôles d'accès physique à l'installation.	✓ ✓	
PE-03-01	CONTRÔLE DE L'ACCÈS PHYSIQUE	• Le fournisseur de services établit des autorisations d'accès physique pour tous les points d'accès physique (y compris les points d'entrée et de sortie désignés) à l'installation où se trouve le système d'information (sauf pour les zones de l'installation officiellement accessibles au public). • Le fournisseur de services vérifie les autorisations d'accès des personnes avant d'autoriser l'accès à l'installation. • Le fournisseur de services contrôle l'accès à l'installation où se trouve le système d'information au moyen de dispositifs d'accès physique ou de gardes. • Le fournisseur de services garde et surveille chaque point d'accès physique de l'installation où se trouve le système d'information 24 heures sur 24 et 7 jours sur 7, et équipe ces points d'accès d'une alarme. • Le fournisseur de services utilise des boîtiers verrouillables pour protéger les composants du système d'information contre tout accès physique non autorisé.		✓ ✓ ✓ ✓ ✓
PE-04	CONTRÔLE D'ACCÈS POUR LES MOYENS DE TRANSMISSION	Le fournisseur de services contrôle l'accès physique aux lignes de distribution et de transmission du système d'information à l'intérieur de ses installations.	✓	
PE-05	CONTRÔLE D'ACCÈS POUR LES ORGANES DE	Le fournisseur de services contrôle l'accès physique aux organes de sortie du système d'information afin d'empêcher	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	SORTIE	toute personne non autorisée d'obtenir les données de sortie.		
PE-06	SURVEILLANCE DE L'ACCÈS PHYSIQUE	• Le fournisseur de services surveille l'accès physique au système d'information afin de détecter les incidents de sécurité physique et d'y réagir. • Le fournisseur de services passe en revue les journaux d'accès physiques au moins une fois par année. • Le fournisseur de services arrime les résultats des examens et des enquêtes à sa capacité d'intervention en cas d'incident.	✓ ✓ ✓	
PE-06-01	SURVEILLANCE DE L'ACCÈS PHYSIQUE	• Le fournisseur de services surveille les alarmes d'intrusion physique en temps réel et le matériel de surveillance.		✓
PE-07	CONTRÔLE DES VISITEURS	• Le fournisseur de services contrôle l'accès physique au système d'information en identifiant les visiteurs avant de leur donner accès à l'installation où se trouve le système d'information, sauf dans les zones accessibles au public.	✓	
PE-07-01	CONTRÔLE DES VISITEURS	• Le fournisseur de services escorte les visiteurs et surveille l'activité de ces derniers, le cas échéant.		✓
PE-08	REGISTRES D'ACCÈS	• Le fournisseur de services tient des registres d'accès à l'installation où se trouve le système d'information (sauf pour les zones de l'installation officiellement ouvertes au public). • Le fournisseur de services passe en revue les registres d'accès des visiteurs au moins une fois par année.	✓ ✓	
PE-08-01	REGISTRES D'ACCÈS	• Le fournisseur de services tient un registre de tous les accès physiques des visiteurs et des personnes autorisées.		✓
PE-09	ÉQUIPEMENT D'ALIMENTATION ET	Le fournisseur de services protège l'équipement d'alimentation et les câbles d'alimentation du système d'information contre	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	CÂBLES D'ALIMENTATION	les dommages et la destruction.		
PE-10	MISE HORS TENSION D'URGENCE	• Le fournisseur de services permet de mettre hors tension le système d'information ou chacun de ses composants en cas d'urgence. • Le fournisseur de services pose des interrupteurs ou autres dispositifs de mise hors tension d'urgence à proximité du système d'information ou de ses composants pour permettre au personnel d'y accéder facilement et en toute sécurité. • Le fournisseur de services protège les dispositifs de mise hors tension d'urgence pour éviter qu'ils ne soient actionnés sans autorisation.	✓ ✓ ✓	
PE-11	ALIMENTATION DE SECOURS	• Le fournisseur de services assure une alimentation sans coupure de courte durée pour faciliter l'arrêt méthodique du système d'information en cas de perte de la source d'alimentation principale.	✓	
PE-12	ÉCLAIRAGE DE SECOURS	• Le fournisseur de services emploie et entretient, pour le système d'information, un éclairage de secours actionné automatiquement en cas d'interruption ou de perturbation du courant. Cet éclairage couvre les sorties d'urgence et les chemins d'évacuation de l'installation.	✓	
PE-13	PROTECTION CONTRE LES INCENDIES	• Le fournisseur de services emploie et entretient des appareils et des systèmes de détection et d'extinction des incendies pour le système d'information, lesquels sont alimentés par une source d'énergie indépendante.	✓	
PE-14	CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ	• Le fournisseur de services maintient à des niveaux acceptables la température et le taux d'humidité de l'installation où se trouve le système d'information.	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
PE-14-01	CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ	• Le fournisseur de services utilise un dispositif de surveillance de la température et de l'humidité qui émet une alarme ou un avis en cas de changements potentiellement dangereux pour le personnel ou le matériel.		✓
PE-15	PROTECTION CONTRE LES DÉGÂTS D'EAU	• Le fournisseur de services protège le système d'information des dégâts causés par les fuites d'eau en prévoyant des robinets d'arrêt principaux qui sont accessibles, qui fonctionnent correctement et dont les principaux membres du personnel connaissent l'existence.	✓	
PE-16	LIVRAISON ET ENLÈVEMENT	• Le fournisseur de services autorise, surveille et contrôle les entrées et sorties des divers types de composants du système d'information et tient des registres des articles en question.	✓	
PE-17	LIEU DE TRAVAIL SECONDAIRE	• Le fournisseur de services : o a recours à des contrôles de sécurité techniques, opérationnels et administratifs pour le système d'information aux lieux de travail secondaires; o évalue l'efficacité des contrôles de sécurité dans les lieux de travail secondaires; o procure aux employés un moyen de communiquer avec le personnel de la sécurité de l'information en cas d'incidents ou de problèmes relatifs à la sécurité.	✓	
PE-18	EMPLACEMENT DES COMPOSANTS DU SYSTÈME D'INFORMATION	Le fournisseur de services positionne les composants du système d'information au sein de l'installation de façon à limiter les dommages éventuels causés par des éléments matériels ou environnementaux et de façon à réduire les possibilités d'accès non autorisé.	✓	

1.12 Planification de la sécurité (PL)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la planification de la sécurité et s'appliquant au service de débit pré-autorisé.

Tableau C-12 : Liste des exigences en matière de planification de la sécurité

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
PL-02	PLAN DE SÉCURITÉ DU SYSTÈME	• Le fournisseur de services prépare un plan de sécurité du système d'information qui : (a) s'inscrit dans l'architecture d'entreprise de l'organisation; (b) délimite de façon explicite les autorisations relatives au système; (c) décrit le contexte d'exploitation du système d'information sous la forme de missions et de processus opérationnels; (d) dresse les catégories de sécurité du système d'information et décrit la logique les justifiant; (e) décrit l'environnement d'exploitation du système d'information; (f) décrit les associations ou les connexions avec d'autres systèmes d'information; (g) résume les exigences en matière de contrôles de sécurité du système; (h) décrit les contrôles de sécurité en place ou prévus pour répondre à ces exigences, y compris les justifications de contrôles personnalisés et complémentaires; (i) est revu et approuvé par l'agent autorisé préalablement à sa mise en œuvre. • Le fournisseur de services revoit le plan de sécurité du système d'information au moins une fois par année; • Le fournisseur de services actualise le plan en fonction des modifications du système ou de son environnement d'exploitation, ainsi qu'en fonction des problèmes relevés au cours de sa mise en œuvre ou de l'évaluation des contrôles de sécurité.	✓ ✓ ✓	
PL-02-01	PLAN DE SÉCURITÉ DU SYSTÈME	• L'organisation : (a) élabore un concept d'opérations (CONOPS) en matière de		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		sécurité applicable au système d'information, concept incluant au minimum : ○ (i) la raison d'être du système, ○ (ii) la description de l'architecture du système, ○ (iii) le calendrier des autorisations de sécurité, ○ (iv) les catégories de sécurité et les facteurs ayant contribué à établir ces catégories; (b) revoit et met à jour le CONOPS au besoin. • Le fournisseur de services élabore et tient à jour l'architecture fonctionnelle du système d'information, architecture décrivant : (a) les interfaces externes, l'information passant par ces interfaces et les mécanismes de protection liés à chacune; (b) les rôles d'utilisateur et les privilèges d'accès de chacun; (c) les exigences en matière de contrôles de sécurité distincts; (d) le type de données traitées, stockées ou transmises par le système d'information, ainsi que les mesures de protection particulières exigées par les lois fédérales ainsi que par les politiques, les directives et les normes du Secrétariat du Conseil du Trésor qui s'appliquent; (e) l'ordre de priorité de la restauration des données ou du rétablissement des services du système d'information.		✓
PL-04	RÈGLES DE CONDUITE	• Le fournisseur de services : ○ établit des règles et les communique à tous les utilisateurs du système d'information afin de définir les responsabilités de ces derniers et la conduite attendue à l'égard des données et de l'utilisation du système d'information; ○ reçoit une attestation signée des utilisateurs confirmant qu'ils ont lu, compris et accepté les règles de conduite avant de leur donner accès aux données et au système d'information; ○ inclut, dans les règles de conduite, des restrictions explicites visant l'utilisation des sites de réseaux sociaux, la publication de renseignements sur des sites Web commerciaux et le partage des renseignements sur les comptes du système	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		d'information.		
PL-06	PLANIFICATION DES ACTIVITÉS LIÉES À LA SÉCURITÉ	• Le fournisseur de services planifie et coordonne les activités liées à la sécurité qui touchent le système d'information avant de les réaliser, de façon à réduire les répercussions sur ses propres activités (c'est-à-dire sa mission, ses fonctions, son image et sa réputation), sur ses biens et sur les personnes.	✓	

1.13 Évaluation des risques (RA)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de l'évaluation des risques et s'appliquant au service de débit pré-autorisé.

Tableau C-13 : Liste des exigences en matière d'évaluation des risques

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
RA-02	CATÉGORISATION DE SÉCURITÉ	• Le fournisseur de services catégorise les données et le système d'information conformément aux lois du gouvernement du Canada et aux politiques, directives et normes du SCT qui s'appliquent. • Le fournisseur de services consigne les résultats de la catégorisation de sécurité (y compris les justifications) dans le plan de sécurité du système d'information. • Le fournisseur de services veille à ce que la décision relative à la catégorisation de sécurité soit examinée et approuvée par l'agent approbateur ou son représentant officiel.	✓ ✓ ✓	
RA-03	ÉVALUATION DES RISQUES	• Le fournisseur de services évalue les risques, notamment la probabilité et l'ampleur des dommages engendrés par un accès non autorisé ou l'utilisation, la divulgation, la perturbation, la modification ou la destruction du système d'information et des données qu'il traite, stocke ou transmet, conformément à la *Norme de sécurité relative à l'organisation et l'administration* du SCT. • Le fournisseur de services met à jour l'évaluation des risques au moins une fois par année ou chaque fois que des modifications importantes sont apportées au système d'information ou à l'environnement d'exploitation (y compris la détermination des nouvelles menaces et failles) ou lorsque d'autres conditions sont susceptibles d'avoir une incidence sur la sécurité du système.	✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
RA-05	ANALYSE DE VULNÉRABILITÉ	• Le fournisseur de services analyse les vulnérabilités du système d'information et des applications hébergées selon le processus défini par l'organisation et lorsque de nouvelles vulnérabilités susceptibles de toucher le système ou les applications sont repérées et signalées. • Le fournisseur de services emploie des outils et des techniques d'analyse qui favorisent l'interopérabilité entre les outils et qui automatisent une partie du processus de gestion des vulnérabilités selon des normes visant : (a) l'énumération des plateformes, des failles logicielles et des configurations incorrectes; (b) le formatage et l'élaboration de listes de vérification et de procédures d'essai transparentes; (c) la mesure de l'incidence de la vulnérabilité. • Le fournisseur de services analyse les rapports de vulnérabilité et les conclusions des évaluations de contrôle de la sécurité. • Le fournisseur de services remédie aux vulnérabilités manifestes conformément à l'évaluation des risques effectuée par un fournisseur de services. • Le fournisseur de services communique les renseignements obtenus au cours de l'analyse de vulnérabilité et des évaluations de contrôle de la sécurité aux membres désignés de son personnel afin de contribuer à corriger des vulnérabilités semblables dans d'autres systèmes d'information (failles ou lacunes systémiques).	✓ ✓ ✓ ✓ ✓	
RA-05-01	ANALYSE DE VULNÉRABILITÉ	• Le fournisseur de services emploie des outils d'analyse de vulnérabilité capables de mettre à jour rapidement la liste des vulnérabilités repérées dans le système d'information. • Le fournisseur de services met à jour la liste des vulnérabilités repérées lors de l'analyse du système d'information au moins une fois par année ou lorsque de nouvelles vulnérabilités sont repérées et signalées.		✓ ✓

1.14 Acquisition du système et des services (SA)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à l'acquisition du système et des services, et s'appliquant au service de débit pré-autorisé.

Tableau C-14 : Liste des exigences en matière d'acquisition du système et des services

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
SA-02	AFFECTATION DES RESSOURCES	• Le fournisseur de services prévoit, dans la planification de la mission et des processus opérationnels, les exigences en matière de contrôles de sécurité du système d'information. • Le fournisseur de services précise, consigne et affecte les ressources nécessaires pour protéger le système d'information dans le cadre de son processus de planification des immobilisations et de contrôle des investissements. • Le fournisseur de services prévoit un élément distinct pour la sécurité de l'information dans ses documents de programmation et d'établissement du budget.	✓ ✓ ✓	
SA-03	AIDE AU CYCLE DE VIE	• Le fournisseur de services gère le système d'information selon une méthode du cycle de développement des systèmes qui tient compte de la sécurité de l'information. • Le fournisseur de services définit et consigne les rôles et les responsabilités en matière de sécurité du système d'information tout au long du cycle de développement du système. • Le fournisseur de services nomme les personnes qui assument des rôles et des responsabilités liés à la sécurité du système d'information.	✓ ✓ ✓	
SA-04	ACQUISITIONS	• Le fournisseur de services inclut de manière explicite ou par renvoi, dans les contrats d'acquisition du système d'information, des exigences et/ou des caractéristiques fonctionnelles en matière de sécurité fondées sur le risque évalué ainsi que sur les lois fédérales et les politiques, les	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		directives et les normes du Secrétariat du Conseil du Trésor qui s'appliquent. • Le fournisseur de services inclut de manière explicite ou par renvoi, dans les contrats d'acquisition du système d'information, des exigences ou des caractéristiques en matière de documents relatifs à la sécurité fondées sur le risque évalué ainsi que sur la *Norme de sécurité et de gestion des marchés* du Secrétariat du Conseil du Trésor. • Le fournisseur de services inclut de manière explicite ou par renvoi, dans les contrats d'acquisition du système d'information, des exigences ou des caractéristiques en matière d'élaboration et d'évaluation fondées sur le risque évalué ainsi que sur les lois fédérales et les politiques, les directives et les normes du Secrétariat du Conseil du Trésor qui s'appliquent.	✓ ✓	
SA-04-01	ACQUISITIONS	• Le fournisseur de services exige, dans les documents d'acquisition que les fournisseurs et les autres fournisseurs de services fournissent, de l'information décrivant les caractéristiques fonctionnelles des contrôles de sécurité qui seront utilisés dans le système d'information, ses composants et ses services. Cette information doit être suffisamment détaillée pour qu'il soit possible d'analyser et de mettre à l'essai les contrôles. • Le fournisseur de services exige, dans les documents d'acquisition, que les composants du système d'information soient, à la livraison, configurés de façon sécuritaire, que la configuration en question soit mise par écrit et qu'elle soit employée par défaut pour les réinstallations ou les mises à niveau des logiciels.		✓ ✓
SA-05	DOCUMENTATION DU SYSTÈME D'INFORMATION	• Le fournisseur de services obtient, protège s'il y a lieu, et communique au personnel autorisé la documentation destinée à l'administrateur du système d'information et décrivant : o la configuration, l'installation et l'exploitation	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		sécurisées du système d'information; ○ l'utilisation et la maintenance efficaces des options et des fonctions de sécurité; ○ les vulnérabilités connues en ce qui concerne la configuration et l'utilisation des fonctions d'administration (fonctions privilégiées); ○ les options et fonctions de sécurité accessibles aux utilisateurs et leur utilisation efficace; ○ 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; ○ les responsabilités des utilisateurs à l'égard de la sécurité des données et du système d'information.		
SA-06	RESTRICTIONS D'UTILISATION DES LOGICIELS	• Le fournisseur de services utilise les logiciels et la documentation connexe conformément aux ententes contractuelles et à la loi sur le droit d'auteur.	✓	
SA-07	LOGICIELS INSTALLÉS PAR LES UTILISATEURS	• Le fournisseur de services applique des règles explicites encadrant l'installation de logiciels par les utilisateurs.	✓	
SA-08	PRINCIPES TECHNIQUES DE SÉCURITÉ	• Le fournisseur de services applique des principes techniques de sécurité des systèmes d'information pour la spécification, la conception, le développement, la mise en œuvre et la modification du système d'information.	✓	
SA-09	SERVICES INFORMATIQUES EXTERNES	• Le fournisseur de services : ○ exige que les fournisseurs de services informatiques externes se conforment aux exigences de contrôle de la sécurité informatique du fournisseur de services et utilisent des contrôles de sécurité appropriés, conformément à la *Norme de sécurité et de gestion des marchés* du SCT; ○ définit et consigne les rôles et les responsabilités	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		du gouvernement à titre de superviseur et d'utilisateur final en ce qui concerne les services informatiques externes; ○ surveille la conformité des contrôles de sécurité effectués par les fournisseurs de services externes.		
SA-09-01	SERVICES INFORMATIQUES EXTERNES	• Le fournisseur de services : (a) évalue les risques avant d'acquérir ou d'impartir des services spécialisés de sécurité de l'information; (b) veille à ce que l'acquisition ou l'impartition de services spécialisés de sécurité de l'information soit approuvée par un haut responsable à son service.		✓

1.15 Isolement de la fonction de sécurité (SC)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à l'isolement de la fonction de sécurité et s'appliquant au service de débit pré-autorisé.

Tableau C-15 : Liste des exigences en matière d'isolement de la fonction de sécurité

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
SC-02	SEGMENTATION DES APPLICATIONS	• Dans le système d'information, les fonctions destinées aux utilisateurs (y compris les services de l'interface utilisateur) sont séparées des fonctions de gestion.	✓	
SC-02-01	SEGMENTATION DES APPLICATIONS	• Le système d'information empêche l'affichage des fonctions de gestion dans l'interface destinée aux utilisateurs ordinaires (sans privilèges).		✓
SC-05	PROTECTION CONTRE LE REFUS DE SERVICE	• Le système d'information prévient ou limite les répercussions des divers types d'attaques entraînant un refus de service.	✓	
SC-05-01	PROTECTION CONTRE LE REFUS DE SERVICE	• Le système d'information gère la capacité ou la largeur de bande excédentaire et toute autre redondance pour limiter les répercussions des attaques entraînant un refus de service par inondation.		✓
SC-07	PROTECTION DES FRONTIÈRES	• Le système d'information : ○ surveille et contrôle les communications à sa périphérie externe et à ses principales frontières internes; ○ se connecte aux réseaux ou aux systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées comprenant des dispositifs de protection des frontières installés selon une architecture de sécurité de fournisseur de services.	✓	
SC-07-01	PROTECTION DES	• Le fournisseur de services :		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	FRONTIÈRES	○ répartit physiquement les composants du système d'information accessibles au public dans des sous-réseaux séparés disposant d'interfaces réseau physiques distinctes; ○ limite le nombre de points d'accès au système d'information afin de permettre une surveillance plus complète des communications entrantes et sortantes et du trafic sur le réseau; ○ met en œuvre une interface gérée pour chacun des services externes de télécommunication; ○ établit une politique sur le flux du trafic pour chaque interface gérée; ○ emploie des contrôles de sécurité au besoin pour préserver la confidentialité et l'intégrité des données transmises; ○ met par écrit chaque exception à la politique sur le flux du trafic en indiquant la mission ou le besoin opérationnel correspondant et sa durée; ○ examine au moins une fois par année les exceptions à la politique sur le flux du trafic; ○ supprime les exceptions à la politique sur le flux du trafic qui ne sont plus justifiées par une mission ou un besoin opérationnel explicite; ○ empêche la sortie non autorisée de données à l'extérieur des frontières du système d'information ou toute communication non autorisée à travers ces frontières en cas de défaillance des mécanismes de protection des frontières; ○ isole les outils, mécanismes et composants de soutien assurant la sécurité de l'information des autres composants internes du système d'information au moyen de sous-réseaux physiquement distincts comprenant des interfaces gérées avec d'autres parties du système.		

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		• Le système d'information : ○ s'interrompt par mesure préventive en cas de défaillance des mécanismes de protection des frontières; ○ bloque par défaut le trafic réseau aux interfaces gérées et surveille les utilisateurs internes (ou les programmes malveillants) qui représentent une menace pour les systèmes d'information externes; ○ contrôle les communications entrantes afin de s'assurer qu'elles proviennent d'une source autorisée et qu'elles sont acheminées vers une destination autorisée; ○ applique des mécanismes de protection des frontières en mode hôte pour les serveurs, les postes de travail et les appareils mobiles; ○ empêche des appareils distants ayant établi une connexion non éloignée avec le système de communiquer en dehors de cette voie de communication avec des ressources de réseaux externes; ○ achemine le trafic des communications internes vers des réseaux externes par l'intermédiaire de serveurs mandataires authentifiés au sein des interfaces gérées des dispositifs de protection des limites; ○ bloque par défaut le trafic réseau aux interfaces gérées et ne le permet que par exception (bloquer tout et autoriser par exception); ○ empêche l'accès du public aux réseaux internes du fournisseur de services sauf lorsque cet accès se fait par l'intermédiaire d'interfaces gérées faisant appel à des dispositifs de protection des frontières.		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
SC-08	INTÉGRITÉ DES TRANSMISSIONS	• Le système d'information préserve l'intégrité des données transmises.	✓	
SC-08-01	INTÉGRITÉ DES TRANSMISSIONS	• Le fournisseur de services emploie des mécanismes cryptographiques pour repérer les modifications des données durant les transmissions, à moins que ces dernières soient protégées par d'autres mesures physiques. Le procédé cryptographique doit être conforme aux exigences de la mesure de contrôle SC-13.		✓
SC-09	CONFIDENTIALITÉ DES TRANSMISSIONS	• Le système d'information préserve la confidentialité des données transmises.	✓	
SC-09-01	CONFIDENTIALITÉ DES TRANSMISSIONS	• Le fournisseur de services emploie des mécanismes cryptographiques pour prévenir la divulgation non autorisée des données durant les transmissions, à moins que ces dernières soient protégées par d'autres mesures physiques définies par l'organisation. Le procédé cryptographique doit être conforme aux exigences de la mesure de contrôle SC-13.		✓
SC-10	DÉCONNEXION DU RÉSEAU	• Le système d'information coupe la connexion réseau associée à une session de transmission à la fin de ladite session ou au terme d'une période d'inactivité réglable dans le système.	✓	
SC-12	CRÉATION ET GESTION D'UNE CLÉ CRYPTOGRAPHIQUE	• Le fournisseur de services crée et gère des clés cryptographiques pour les besoins de cryptographie au sein du système d'information.	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
SC-12-01	CRÉATION ET GESTION D'UNE CLÉ CRYPTOGRAPHIQUE	• Le fournisseur de services tient les renseignements à disposition en cas de perte des clés cryptographique par les utilisateurs.		✓
SC-13	UTILISATION DE LA CRYPTOGRAPHIE	• Le système d'information met en œuvre des protections cryptographiques au moyen de systèmes cryptographiques conformes aux lois du gouvernement du Canada et aux politiques, directives et normes du SCT qui s'appliquent.	✓	
SC-13-01	UTILISATION DE LA CRYPTOGRAPHIE	• Le fournisseur de services emploie une cryptographie validée selon le Programme de validation des modules cryptographiques et approuvée par le CSTC pour mettre en œuvre les signatures numériques.		✓
SC-14	PROTECTION DE L'ACCÈS PUBLIC	• Le système d'information préserve l'intégrité et la disponibilité de l'information et des applications accessibles au public.	✓	
SC-17	CERTIFICATS DE L'INFRASTRUCTURE À CLÉS PUBLIQUES	• Le fournisseur de services délivre des certificats de clés publiques en vertu d'une politique de certificat ou obtient des certificats à clés publiques en vertu de la politique de certificat pertinente d'un fournisseur de services approuvé.	✓	
SC-19	VOIX SUR IP	• Le fournisseur de services : ○ établit des restrictions d'utilisation et des directives de mise en œuvre pour les technologies de voix sur IP en fonction du potentiel d'endommagement du système d'information en cas d'utilisation malveillante; ○ autorise, surveille et contrôle l'utilisation de la voix sur IP au sein du système d'information.	✓	
SC-22	ARCHITECTURE ET DIMENSIONNEMENT POUR	Les systèmes d'information qui fournissent collectivement un service de résolution du nom et de l'adresse pour une	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	LE SERVICE DE RÉSOLUTION DU NOM ET DE L'ADRESSE	organisation sont insensibles aux défaillances et appliquent une séparation des rôles internes et externes.		
SC-23	AUTHENTICITÉ DES SESSIONS	• Le système d'information possède des mécanismes pour protéger l'authenticité des sessions de transmission.	✓	
SC-23-01	AUTHENTICITÉ DES SESSIONS	• Le système d'information : ○ annule les identifiants de session lors de la fermeture de session par l'utilisateur ou lors de tout autre type de fermeture de session; ○ possède une capacité de fermeture de session facilement observable lorsque l'authentification est requise pour accéder aux pages Web; ○ génère un identificateur de session unique pour chaque session et reconnaît uniquement les identificateurs de session qu'il génère; ○ génère les identificateurs de session unique de façon aléatoire.		✓
SC-28	PROTECTION DES DONNÉES STATIQUES	Le système d'information préserve la confidentialité et l'intégrité des données statiques.	✓	

1.16 Intégrité du système et de l'information (SI)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à l'intégrité du système et de l'information et s'appliquant au service de débit pré-autorisé.

Tableau C-16 : Liste des exigences en matière d'intégrité du système et de l'information

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
SI-02	CORRECTION DES FAILLES	• Le fournisseur de services repère, signale et corrige les failles du système d'information.	✓	
SI-03	PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS	• Le fournisseur de services emploie des mécanismes de protection contre les programmes malveillants aux points d'entrée et de sortie du système d'information ainsi que sur les postes de travail, les serveurs et les appareils informatiques mobiles connectés au réseau afin de détecter et d'éliminer les programmes malveillants : (a) transmis par les courriels, les pièces jointes aux courriels, les accès à Internet, les supports d'information amovibles ou d'autres moyens courants; (b) insérés par l'exploitation des vulnérabilités du système d'information. • Le fournisseur de services met à jour les mécanismes de protection contre les programmes malveillants (y compris les définitions des signatures) chaque fois qu'une nouvelle version est disponible, conformément à la politique et aux procédures de gestion de la configuration que l'organisation a définies. • Le fournisseur de services configure les mécanismes de protection contre les programmes malveillants de façon à : (a) effectuer des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au moment de leur chargement, de leur ouverture ou de leur exécution, conformément à sa politique de sécurité; (b)	✓ ✓ ✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		☒ bloquer les programmes malveillants, ☒ mettre les programmes malveillants en quarantaine, ☒ envoyer une alerte à l'administrateur, lorsque des programmes malveillants sont détectés. • Le fournisseur de services prend en compte la réception de faux positifs dans le cadre de la détection et de la suppression des programmes malveillants ainsi que les répercussions potentielles que ceux-ci peuvent avoir sur la disponibilité du système d'information.	✓	
SI-03-01	PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS	• Le fournisseur de services : ○ centralise la gestion des mécanismes de protection contre les programmes malveillants; ○ empêche les utilisateurs d'introduire des supports amovibles dans le système d'information; ○ met à l'essai les mécanismes de protection contre les programmes malveillants en introduisant dans le système d'information un jeu d'essai connu, inoffensif et incapable de se propager. Il vérifie ensuite si la détection du jeu d'essai et le signalement de l'incident connexe ont bien lieu. Il doit accomplir cette tâche au besoin, au moins une fois par année. • Le système d'information : ○ met automatiquement à jour les mécanismes de protection contre les programmes malveillants (y compris les définitions des signatures); ○ empêche les utilisateurs non privilégiés de contourner les capacités de protection contre les programmes malveillants; ○ met à jour les mécanismes de protection contre les programmes malveillants uniquement lorsqu'un utilisateur privilégié lui en donne l'instruction.		✓ ✓
SI-04	SURVEILLANCE DU	• Le fournisseur de services :		

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	SYSTÈME D'INFORMATION	○ surveille les événements qui se produisent dans le système d'information conformément aux objectifs de surveillance et détecte les attaques du système d'information; ○ repère les utilisations non autorisées du système d'information; ○ déploie des dispositifs de surveillance : (i) de façon stratégique au sein du système d'information pour recueillir les renseignements jugés essentiels par l'organisation, et (ii) en des endroits appropriés au sein du système pour suivre certains types de transactions ayant un intérêt pour lui; ○ augmente le niveau de surveillance du système d'information lorsqu'on suppose un risque accru pour les activités et les biens de fournisseurs de services, pour les personnes, pour d'autres organisations ou pour le Canada selon les renseignements concernant le respect des lois, les renseignements secrets ou d'autres sources de renseignements crédibles; ○ obtient 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; ○ emploie des outils pour appuyer l'analyse en temps réel des événements; ○ protège les renseignements obtenus grâce aux outils de surveillance des intrusions contre les accès non autorisés, les modifications et la suppression; ○ met à l'essai les outils de surveillance des intrusions au moins une fois par année; ○ fait en sorte que le trafic chiffré soit visible pour les outils de surveillance du système d'information; ○ analyse les transmissions sortantes aux frontières externes du système (c.-à-d. le périmètre du système) et, s'il y a lieu, aux points internes choisis		

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		au sein du système (p. ex. sous-réseaux, sous-systèmes) pour déceler les anomalies; ○ emploie des mécanismes pour avertir le personnel de sécurité des activités inhabituelles ou non autorisées pouvant avoir des répercussions sur la sécurité entraînant une alerte; ○ analyse les types de transmissions et d'événements du système d'information; ○ élabore des profils représentant les types de trafic et les événements courants; ○ utilise les profils de trafic et d'événements pour régler les dispositifs de surveillance du système et réduire ainsi le nombre de faux positifs et de faux négatifs; ○ emploie un système de détection d'intrusion sans fil pour déceler les appareils sans fil indésirables et les compromissions ou intrusions potentielles au sein du système d'information; ○ emploie un système de détection d'intrusion pour surveiller le trafic des transmissions sans fil lorsque ce trafic passe des réseaux sans fil aux réseaux filaires. • Le système d'information : ○ surveille les transmissions entrantes et sortantes afin de déceler les activités ou conditions inhabituelles ou non autorisées; ○ fournit des alertes en temps quasi réel lorsque des signes de compromission ou de compromission potentielle se manifestent; ○ empêche les utilisateurs non privilégiés de contourner les capacités de détection et de prévention des intrusions; ○ avertit les membres du personnel chargés de la réaction aux incidents (membres désignés par leur nom ou leur fonction) des événements suspects et applique les mesures les moins perturbatrices afin	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		de mettre fin aux événements suspects.		
SI-05	ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ	• Le fournisseur de services : ○ reçoit régulièrement des alertes, des conseils et des directives de sécurité pour le système d'information de la part d'organisations externes désignées; ○ génère des alertes, des conseils et des directives internes concernant la sécurité s'il estime que cela est nécessaire; ○ communique les alertes, les conseils et les directives de sécurité aux membres du personnel (désignés par leur nom ou par leur rôle); ○ applique les directives de sécurité conformément aux délais établis ou bien avertit l'organisation émettrice du degré de non-conformité.	✓	
SI-07	INTÉGRITÉ DES LOGICIELS ET DES DONNÉES	• Le système d'information détecte les modifications non autorisées apportées aux logiciels et aux données.	✓	
SI-07-01	INTÉGRITÉ DES LOGICIELS ET DES DONNÉES	• Le fournisseur de services : ○ réévalue l'intégrité des logiciels et des données en effectuant une analyse de l'intégrité du système d'information au moins une fois par année; ○ emploie des outils automatisés qui avisent les personnes désignées lorsqu'ils détectent des écarts lors de la vérification de l'intégrité; ○ emploie des outils de vérification de l'intégrité dont la gestion est centralisée. • Le fournisseur de services exige l'utilisation d'emballages inviolables pour les composants du système d'information pendant : ☒ le transport depuis son site au site d'exploitation, ☒ le fonctionnement.		✓ ✓
SI-08	PROTECTION CONTRE LES POURRIELS	• Le fournisseur de services : ○ emploie des mécanismes de protection contre les	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		pourriels aux points d'entrée et de sortie du système d'information ainsi que sur les postes de travail, les serveurs ou les appareils informatiques mobiles connectés au réseau afin de détecter et d'éliminer les messages non sollicités transmis par les courriels, les pièces jointes aux courriels, les accès Internet ou d'autres moyens courants; ○ met à jour les mécanismes de protection contre les pourriels (y compris les définitions des signatures) chaque fois qu'une nouvelle version est disponible, conformément à sa politique et à ses procédures de gestion de la configuration.		
SI-08-01	PROTECTION CONTRE LES POURRIELS	• Le fournisseur de services centralise la gestion des mécanismes de protection contre les pourriels. • Le système d'information met à jour automatiquement les mécanismes de protection contre les pourriels (y compris les définitions des signatures).		✓ ✓
SI-09	RESTRICTIONS CONCERNANT L'ENTRÉE DE DONNÉES	• Le fournisseur de services restreint la possibilité d'entrer des données dans le système d'information au personnel autorisé.	✓	
SI-10	VALIDATION DES ENTRÉES DE DONNÉES	• Le système d'information vérifie la validité des entrées de données.	✓	
SI-11	TRAITEMENT DES ERREURS	• Le système d'information : ○ détecte les erreurs pouvant avoir une incidence sur la sécurité; ○ génère des messages d'erreur qui fournissent les renseignements nécessaires aux mesures correctives sans révéler de renseignements de nature délicate ou potentiellement dangereux dans les relevés d'erreurs et les messages administratifs, qui pourraient être exploités par des adversaires;	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ communique les messages d'erreur uniquement au personnel autorisé.		
SI-12	TRAITEMENT ET RÉTENTION DES SORTIES DE DONNÉES	Le fournisseur de services traite et retient à la fois les données dans le système d'information et les sorties de données conformément aux lois du gouvernement du Canada et aux politiques, directives et normes du SCT qui s'appliquent.	✓	

1.17 Sensibilisation et formation (AT)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées à la sensibilisation et à la formation et s'appliquant au service de débit pré-autorisé.

Tableau C-17 : Liste des exigences en matière de sensibilisation et de formation

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
AT-02	SENSIBILISATION À LA SÉCURITÉ	Le fournisseur de services donne une formation de sensibilisation à la sécurité de base à tous les utilisateurs du système d'information (y compris les gestionnaires, les cadres supérieurs et les fournisseurs de services) dans la cadre de la formation initiale destinée aux nouveaux utilisateurs, lorsque des modifications au système l'exigent et annuellement par la suite.	✓	
AT-03	FORMATION SUR LA SÉCURITÉ	Le fournisseur de services donne une formation sur la sécurité axée sur les rôles : (i) avant d'autoriser l'accès au système ou avant l'exécution des tâches assignées; (ii) lorsque des modifications du système l'exigent; (iii) au moins une fois par année par la suite.	✓	
AT-04	DOSSIERS DE FORMATION SUR LA SÉCURITÉ	• Le fournisseur de services : o consigne et surveille les activités individuelles de formation sur la sécurité du système d'information, y compris la formation de sensibilisation à la sécurité de base et la formation axée sur la sécurité du système d'information; o conserve les dossiers de formation individuels pour une période déterminée par sa politique interne de formation.	✓	

1.18 Sécurité du personnel (PS)

Le tableau ci-dessous énumère les exigences en matière de sécurité de la TI liées au domaine de la sécurité du personnel et s'appliquant au service de débit pré-autorisé.

Tableau C-18 : Liste des exigences en matière de sécurité du personnel

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
PS-03	ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL	• Le fournisseur de services enquête sur les personnes avant de leur donner accès au système d'information conformément à la *Norme sur la sécurité du personnel* du SCT. • Le fournisseur de services mène une deuxième enquête sur les personnes lorsque les conditions l'exigent.	✓ ✓	
PS-04	LICENCIEMENT D'UN MEMBRE DU PERSONNEL	• Le fournisseur de services annule l'accès au système d'information lors du licenciement d'un employé. • Le fournisseur de services effectue une entrevue de départ lors du licenciement d'un employé. • Le fournisseur de services récupère tous les biens liés à la sécurité de son système d'information lors du licenciement d'un employé.	✓	
PS-06	ENTENTES D'ACCÈS	• Le fournisseur de services veille à ce que les personnes devant accéder à ses données et à ses systèmes d'information signent les ententes d'accès nécessaires avant d'obtenir cet accès. • Le fournisseur de services examine et met à jour les ententes d'accès au moins une fois par année.	✓ ✓	
PS-06-01	ENTENTES D'ACCÈS	• Le fournisseur de services veille à ce que l'accès à l'information faisant l'objet de mesures de protection spéciales ne soit accordé qu'aux personnes : (a) ayant une autorisation d'accès valide au titre des fonctions gouvernementales officielles qui leur ont été		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		attribuées; (b) répondant aux critères connexes en matière de sécurité du personnel.		
PS-07	SÉCURITÉ DU PERSONNEL ASSURÉE PAR UN TIERS	• Le fournisseur de services définit les exigences de contrôle de la sécurité du personnel, dont les rôles et les responsabilités des fournisseurs tiers. • Le fournisseur de services met par écrit les exigences de contrôle de la sécurité du personnel. • Le fournisseur de services surveille la conformité du fournisseur. • Le fournisseur de services mène une enquête de sécurité sur les organisations et les personnes du secteur privé qui ont accès aux renseignements et aux biens protégés et classifiés, conformément à la *Norme sur la sécurité du personnel* du SCT. • Le fournisseur de services définit explicitement les rôles et les responsabilités du gouvernement à titre de superviseur et d'utilisateur final en ce qui concerne les services fournis par des tiers, conformément à la *Norme de sécurité et de gestion des marchés* du SCT.	✓ ✓ ✓ ✓ ✓	
PS-08	SANCTIONS CONTRE LE PERSONNEL	• Le fournisseur de services suit une procédure officielle pour prendre des sanctions contre le personnel contrevenant aux procédures et aux politiques établies en matière de sécurité de l'information.	✓	