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
EFT REMITTANCE SERVICE

Solicitation No. - N° de l'invitation	**Date**
EN891-132308/A	2013-04-22

Client Reference No. - N° de référence du client
20132308

GETS Reference No. - N° de référence de SEAG
PW-$$ZG-410-25983

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
410zg.EN891-132308	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2013-05-22

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

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:

Specified Herein
Précisé dans les présentes

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, ainsi que la méthode de sélection;

Partie 5 Attestations : comprend les attestations à fournir;

Partie 6 Exigences relatives à la sécurité et exigences financières: 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 et les attestations préalables à l'attribution du contrat.

Les annexes comprennent l'énoncé des travaux, la base de paiement et la liste de vérification des exigences relatives à la sécurité.

2. Sommaire

2.1 Travaux publics et Services gouvernementaux Canada (TPSGC), au nom du Receveur général du Canada, cherche à conclure un contrat officiel avec un seul fournisseur de services, pour le traitement des transferts électroniques de fonds (TEF). Le service doit couvrir les paiements libellés en dollars canadiens effectués au gouvernement par dépôt direct et par virement télégraphique.

À l'heure actuelle, cinquante-quatre (54) ministères et organismes fédéraux, pour un total de quatre-vingt-huit (88) bureaux ministériels, acceptent les dépôts directs et les virements télégraphiques.

La période initiale du contrat sera d'une durée de trois (3) ans à compter de la date d'attribution du contrat. Le contrat comprendra une option irrévocable permettant d'en prolonger la durée d'au plus deux (2) périodes d'une (1) année chacune et une période de transition de six (6) mois, selon les mêmes termes et conditions.

2.2 Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7, Clauses du contrat subséquent. Les soumissionnaires devraient consulter le document " Exigences de sécurité pour 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.

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 (2012-11-19), Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

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 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 (2 copies papier*)*; et
Section III: Attestations et documentation connexe (1 copie 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 .

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

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 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 des Taxes aplicables doit être indiqué séparément.

1.2 Les soumissionnaires doivent soumettre leurs prix et taux FAB destination; les droits de douane et les taxes d'accise canadiens compris, s'il y a lieu; et les Taxes applicables exclues.

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 les attestations exigées à la Partie 5 et la documentation connexe dans la Section III de leur soumission.

PIÈCE JOINTE 1 DE LA PARTIE 3
BARÈME DE PRIX

Le soumissionnaire doit remplir ce barème de prix et l'inclure dans sa soumission financière. Au minimum, le soumissionnaire doit répondre à ce barème de prix en indiquant dans sa soumission financière, pour chacune des périodes précisées ci-dessous, les frais fermes tout compris (en dollars canadiens) qu'il propose pour chaque catégorie identifiée.

Les données volumétriques figurant dans ce document ne représentent pas un engagement de la part du Canada selon lequel l'utilisation future par le Canada des services décrits dans la demande de soumissions sera conforme à ces données.

Voici les seules catégories de frais qui peuvent être proposées :

A. frais par transaction de TEF;
B. frais uniques pour l'établissement de bureaux ministériels;
C. frais mensuels pour l'accès en ligne des utilisateurs ministériels;
D. frais accessoires applicables aux transactions d'une valeur égale ou supérieure à 50 M$.

Remarque : Tous les autres coûts engagés par le 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 catégories (A, B, C et D) décrites ci-dessous.
Les cellules à fond gris ne sont fournies qu'à des fins d'évaluation; le soumissionnaire ne doit pas les remplir.

A. Frais de transaction de TEF

Il s'agit des frais fermes tout compris applicables à chaque transaction de dépôt direct et de virement télégraphique figurant dans le relevé bancaire électronique quotidien EDI 821 sur les TEF. Les frais de transaction tout compris doivent tenir compte de toutes les exigences relatives au traitement et à l'établissement de rapports.

Directives

a) Le soumissionnaire doit indiquer clairement les frais de transaction fermes tout compris applicables à chaque fourchette annuelle des volumes et à chaque année dans les lignes 1 à 3 des tableaux A1 et A2 (colonnes B, D, F, H et J).

b) Si un soumissionnaire souhaite offrir des frais fixes, sans égard au volume, il doit indiquer des frais identiques pour chaque fourchette des volumes dans les tableaux A1 et A2.

c) L'équipe d'évaluation utilisera les données du tableau A3 pour établir le tableau E1 (Sommaire des frais – Prix total évalué). Les frais annuels pondérés applicables aux transactions de TEF seront calculés de la manière suivante : (somme des coefficients de pondération des prix de la fourchette des volumes) x (volumes annuels prévus de dépôts directs) + (somme des coefficients de pondération des prix de la fourchette des volumes) x (volumes annuels prévus de virements télégraphiques). **Le tableau A3 n'est fourni qu'à des fins d'évaluation; le soumissionnaire ne doit pas le remplir.**

Tableau A1 – Dépôts directs

FRAIS DE TRANSACTION FERMES TOUT COMPRIS APPLICABLES AUX DÉPÔTS DIRECTS												
		A	B	C	D	E	F	G	H	I	J	K
	Fourchette annuelle des volumes	**Coefficient de pondération**	**Année 1 - Frais unitaires**	**Frais pondérés (A x B)**	**Année 2 - Frais unitaires**	**Frais pondérés (A x D)**	**Année 3 - Frais unitaires**	**Frais pondérés (A x F)**	**Année d'option 1 - Frais unitaires**	**Frais pondérés (A x H)**	**Année d'option 2 - Frais unitaires**	**Frais pondérés (A x J)**
1	**de 1 à 5 000**	**0,20**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
2	**de 5 000 à 10 000**	**0,50**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
3	**10 001 et +**	**0,30**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
4	**Frais pondérés totaux par transaction (1 + 2 + 3)**			**$**		**$**		**$**		**$**		**$**

Tableau A2 – **Virements télégraphiques**

FRAIS DE TRANSACTION FERMES TOUT COMPRIS APPLICABLES AUX VIREMENTS TÉLÉGRAPHIQUES												
		A	B	C	D	E	F	G	H	I	J	K
	Fourchette annuelle des volumes	**Coefficient de pondération**	**Année 1 - Frais unitaires**	**Frais pondérés (A x B)**	**Année 2 - Frais unitaires**	**Frais pondérés (A x D)**	**Année 3 - Frais unitaires**	**Frais pondérés (A x F)**	**Année d'option 1 - Frais unitaires**	**Frais pondérés (A x H)**	**Année d'option 2 - Frais unitaires**	**Frais pondérés (A x J)**
1	**de 1 à 15 000**	**0,20**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
2	**de 15 000 à 30 000**	**0,50**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
3	**30 001 et +**	**0,30**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
4	**Frais pondérés totaux par transaction (1 + 2 + 3)**			**$**		**$**		**$**		**$**		**$**

Tableau A3 – **Sommaire des frais annuels pondérés applicables aux transactions de TEF**

Le tableau A3 n'est fourni qu'à des fins d'évaluation; le soumissionnaire ne doit pas le remplir.

	FRAIS ANNUELS PONDÉRÉS APPLICABLES AUX TRANSACTIONS DE TEF					
	Catégorie	Année 1	Année 2	Année 3	Année d'option 1	Année d'option 2
1	Volume prévu de dépôts directs	6 197	6 507	6 833	7 174	7 533
2	Frais pondérés totaux par transaction (insérer les valeurs indiquées à la ligne 4 du tableau A1)	**$**	**$**	**$**	**$**	**$**
3	**Frais annuels pondérés pour le dépôt direct** (ligne 1 x ligne 2)	**$**	**$**	**$**	**$**	**$**
4	Volume prévu de virements télégraphiques	19 221	20 182	21 191	22 251	23 363
5	Frais pondérés totaux par transaction (insérer les valeurs indiquées à la ligne 4 du tableau A2)	**$**	**$**	**$**	**$**	**$**
6	**Frais annuels pondérés pour le virement télégraphique** (ligne 4 x ligne 5)	**$**	**$**	**$**	**$**	**$**
7	**Frais annuels pondérés applicables aux transactions de TEF** (ligne 3 + ligne 6)	**$**	**$**	**$**	**$**	**$**

B. Frais d'établissement de bureaux ministériels

Il s'agit de frais uniques qui servent à l'établissement et au maintien de bureaux ministériels ayant la capacité de recevoir des remises de TEF. Le bureau ministériel peut concerner un ministère ou encore une division ou un programme au sein d'un ministère particulier auquel le RG a jugé pertinent d'établir une identité propre aux fins de réception des recettes et de rapports. Ces frais doivent comprendre toutes les activités administratives nécessaires pour que cette capacité soit mise en œuvre.

Directives

a) Le soumissionnaire doit indiquer clairement les frais fermes tout compris applicables à l'établissement de bureaux ministériels pour chaque année du contrat dans la ligne 2 du tableau B1 (colonnes A, B, C, D et E).

b) Les frais annuels estimatifs totaux applicables à l'établissement de bureaux ministériels seront calculés de la manière suivante : (frais uniques tout compris applicables à l'établissement de bureaux ministériels) x (volumes estimatifs annuels de bureaux ministériels à établir). Le résultat de ce calcul sera inscrit dans la ligne 3 du tableau B1.

Tableau B1 – Frais uniques fermes tout compris applicables à l'établissement de bureaux ministériels

FRAIS UNIQUES FERMES TOUT COMPRIS APPLICABLES À L'ÉTABLISSEMENT DE BUREAUX MINISTÉRIELS						
		A	**B**	**C**	**D**	**E**
		Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
1	**Volume estimatif de bureaux ministériels à établir**	100	10	5	5	5
2	**Frais uniques tout compris applicables à l'établissement de bureaux ministériels**	**$**	**$**	**$**	**$**	**$**
3	**Frais annuels totaux estimatifs applicables à l'établissement de bureaux ministériels** (ligne 1 x ligne 2)	**$**	**$**	**$**	**$**	**$**

C. Frais pour l'accès en ligne des utilisateurs ministériels

Il s'agit de frais mensuels applicables à l'établissement et au maintien d'un accès à l'outil de rapports en ligne du soumissionnaire pour les utilisateurs ministériels. Ces frais doivent couvrir toutes les activités administratives nécessaires pour que cette capacité soit mise en œuvre.

Directives

a) Le soumissionnaire doit indiquer clairement les frais d'accès mensuels fermes tout compris par utilisateur applicables à chaque année du contrat dans la ligne 2 du tableau C1 (colonnes A, B, C, D et E).

b) Les frais annuels fermes tout compris pour l'accès en ligne des utilisateurs ministériels seront calculés de la manière suivante : (frais d'accès mensuels fermes tout compris par utilisateur) x (volumes estimatifs d'utilisateurs ministériels) x (12 mois). Le résultat de ce calcul sera inscrit dans la ligne 4 du tableau C1.

Tableau C1 – Frais mensuels tout compris pour l'accès en ligne des utilisateurs ministériels

FRAIS MENSUELS FERMES TOUT COMPRIS POUR L'ACCÈS EN LIGNE DES UTILISATEURS MINISTÉRIELS						
		A	**B**	**C**	**D**	**E**
		Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
1	**Volume estimatif d'utilisateurs ministériels**	225	245	255	265	275
2	**Frais d'accès mensuels fermes tout compris par utilisateur**	**$**	**$**	**$**	**$**	**$**
3	**Nombre de mois**	**12**	**12**	**12**	**12**	**12**
4	**Frais d'accès mensuels** (ligne 1 x ligne 2 x ligne 3)	**$**	**$**	**$**	**$**	**$**

D. Frais accessoires applicables aux transactions d'une valeur égale ou supérieure à 50 M$

Un taux ferme fondé sur des points de base sera appliqué à chaque transaction dont la valeur est égale ou supérieure à 50 M$. Puisque l'entrepreneur doit transférer les fonds au compte du RG ouvert à la Banque du Canada le jour de leur réception, s'ils ont été reçus avant 14 h HAE, ou le jour suivant leur réception, s'ils ont été reçus après 14 h HAE, nous sommes conscients que des frais accessoires pourraient devoir être versés lorsque des paiements de grande valeur sont reçus. C'est pourquoi nous avons prévu une méthode par laquelle l'entrepreneur pourra réclamer des frais accessoires relativement à chaque transaction dont la valeur est égale ou supérieure à 50 M$.

Le taux fondé sur des points de base doit être exprimé par un nombre entier. Par exemple, le chiffre 8 représente 8 points de base.

Directives

a) Le soumissionnaire doit indiquer clairement le taux ferme fondé sur des points de base applicable à chaque année du contrat dans la ligne 2 du

tableau D1 (colonnes A, B, C, D et E).

b) Les frais accessoires annuels tout compris applicables aux transactions dont la valeur est égale ou supérieure à 50 M$ seront calculés de la manière suivante : (taux fondé sur des points de base) x (volume annuel estimatif des transferts d'une valeur égale ou supérieure à 50 M$) ÷ (nombre de jours ouvrables). Le résultat de ce calcul sera inscrit dans la ligne 4 du tableau D1.

a. Dans la formule, le taux fondé sur des points de base sera représenté de la façon suivante : les points de base (8) sont convertis en nombre décimal (0,0008) aux fins du calcul des frais annuels.

b. Il y a 250 jours ouvrables dans une année.

Tableau D1 – **Frais accessoires tout compris applicables aux transactions d'une valeur égale ou supérieure à 50 M$**

FRAIS ACCESSOIRES TOUT COMPRIS APPLICABLES AUX TRANSACTIONS D'UNE VALEUR ÉGALE OU SUPÉRIEURE À 50 M$						
		A	B	C	D	E
		Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
1	**Valeur annuelle prévue** (somme des transactions d'une valeur égale ou supérieure à 50 M$)	**4 079 000 000 $**	**4 283 000 000 $**	**4 497 000 000 $**	**4 722 000 000 $**	**4 958 000 000 $**
2	**Taux ferme tout compris fondé sur des points de base applicable aux transactions dont la valeur est égale ou supérieure à 50 M$**					
3	**Nombre de jours ouvrables**	**250**	**250**	**250**	**250**	**250**
4	**Frais accessoires annuels tout compris** (ligne 1 x ligne 2 ÷ ligne 3)	**$**	**$**	**$**	**$**	**$**

E. Sommaire des frais – Prix total évalué – AUX FINS D'ÉVALUATION SEULEMENT

Le prix total évalué correspondra à la somme des quatre catégories (A, B, C et D) décrites ci-dessus.

Le tableau E1 n'est fourni qu'à des fins d'évaluation; le soumissionnaire ne doit pas le remplir.

Tableau E1 – PRIX TOTAL ÉVALUÉ

		1	2	3	4	5
		Année 1	Année 2	Année 3	Année d'option 1	Année d'option 2
Description de l'élément		Frais annuels	Frais annuels	Frais annuels	Frais annuels	Frais annuels
A	Frais applicables aux transactions de TEF (frais annuels pondérés indiqués à la ligne 7 du tableau A3)	$	$	$	$	$
B	Frais d'établissement de bureaux ministériels (frais annuels indiqués à la ligne 3 du tableau B1)					
C	Frais pour l'accès en ligne des utilisateurs ministériels (frais annuels indiqués à la ligne 4 du tableau C1)	$	$	$	$	$
D	Frais accessoires applicables aux transactions d'une valeur égale ou supérieure à 50 M$ (frais annuels tout compris indiqués à la ligne 4 du tableau D1)	$	$	$	$	$
	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 indiqués aux 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 Critère technique obligatoire

La soumission doit répondre au critère technique obligatoire énoncé ci-dessous. Le soumissionnaire doit fournir la documentation nécessaire pour démontrer sa conformité au critère.

Les soumissions qui ne répondent pas au critère technique obligatoire seront déclarées non recevables.

Critères techniques obligatoires (CTO)

Aux fins des critères techniques obligatoires indiqués ci-dessous, l'expérience du soumissionnaire sera prise en considération.

Numéro	Critère technique obligatoire	Instructions pour la préparation des soumissions
CTO1	À la date de clôture de l'invitation à soumissionner, le soumissionnaire doit être un membre participant du Système de transfert de paiements de grande valeur (STPGV) de l'Association canadienne des paiements (ACP).	Le soumissionnaire devrait produire la preuve de sa participation, par exemple un certificat de participation, un numéro de membre ou une lettre d'acceptation fournie par l'ACP. Le soumissionnaire devrait fournir la documentation nécessaire pour démontrer sa conformité au critère.

PARTIE 5 - ATTESTATIONS

Pour qu'un contrat leur soit attribué, les soumissionnaires doivent fournir les attestations exigées et la documentation connexe. Le Canada déclarera une soumission non recevable si les attestations exigées et la documentation connexe ne sont pas remplies et fournies tel que demandé. Les soumissionnaires devraient inclure les attestations exigées et la documentation connexe 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, de fournir la documentation connexe 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 préalables à l'attribution du contrat

1.1 Code de conduite et attestations - documentation connexe

En présentant une soumission, le soumissionnaire atteste, en vertu de l'article 01 des instructions uniformisées 2003, en son nom et en celui de ses affiliés, qu'il respecte la clause concernant le Code de conduite et attestations, des instructions uniformisées. La documentation connexe requise à cet égard aidera le Canada à confirmer que les attestations sont véridiques.

1.2 Attestations additionnelles 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 - 200 000 $ ou plus

1. En vertu du Programme de contrats fédéraux (PCF), certains fournisseurs, y compris un fournisseur qui est membre d´une coentreprise, soumissionnant pour des contrats du gouvernement fédéral d'une valeur de 200 000 $ ou plus (incluant les Taxes applicables) doivent s'engager officiellement à mettre en oeuvre un programme d'équité en matière d'emploi. Il s'agit d'une condition préalable à l'attribution du contrat. Si le soumissionnaire est assujetti au PCF ou, si le soumissionnaire est une coentreprise et que n'importe lequel des membres de la coentreprise est assujetti au PCF, la preuve de l'engagement du soumissionnaire ou de chaque membre de la coentreprise qui est assujetti au PCF doit être fournie par le soumissionnaire avant l'attribution de tout contrat subséquent découlant de la demande de soumissions.

   Les fournisseurs 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 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.

2. Le soumissionnaire ou, si le soumissionnaire est une coentreprise, n'importe lequel des membres de la coentreprise qui n'est pas visé par les exceptions énumérées aux paragraphes 3.a ou b ci-dessous ou qui n'a pas de numéro d'attestation valide confirmant son adhésion au PCFdoit télécopier (819-953-8768) un exemplaire signé du formulaire LAB 1168, Attestation d'engagement pour la mise en oeuvre de l'équité en matière d'emploi, à la Direction générale du travail de RHDCC.

3. 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 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 $ (incluant les Taxes applicables) ou plus. Dans ce cas, une attestation d'engagement dûment signée est jointe;

   d. ( ) est assujetti au PCF, 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, 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

Le soumissionnaire doit fournir une répondre à la question suivante:

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension? **OUI ( ) NON ( )**; et

si la réponse est oui, le soumissionnaire doit fournir l'information suivante pour tous les anciens fonctionnaires touchant une pension, le cas échéant:

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

En fournissant cette information, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension en vertu de la LPFP, soit publié dans les rapports de

divulgation proactive des marchés, sur les sites Web des ministères, et ce conformément à l'Avis sur la Politique des marchés:2012-2 et aux Lignes directrices sur la divulgation des marchés .

Programme de réduction des effectifs

Le soumissionnaire doit fournir une répondre à la question suivante:

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 ( )** ; et

si la réponse est 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 les Taxes applicables.

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 limité aux services canadiens.

Le soumissionnaire atteste que :

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

1.4 Participant du STPGV de l'ACP

Si un contrat est octroyé suite à la demande de soumissions, le soumissionnaire atteste qu'il doit conserver son statut de participant du Système de transfert de paiements de grande valeur (STPGV) de l'Association canadienne des paiements (ACP) durant la période d'exécution du contrat et de toute autre période optionnelle de prolongation, y compris la période de transition.

PARTIE 6 - EXIGENCES RELATIVES À LA SÉCURITÉ ET EXIGENCES FINANCIÈRES

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'indiqué 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'indiqué à la Partie 7 - Clauses du contrat subséquent;

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;

d) le lieu proposé par le soumissionnaire pour la réalisation des travaux ou la sauvegarde des documents doit satisfaire aux exigences relatives à la sécurité précisées à la Partie 7 - Clauses du contrat subséquent; et

e) le soumissionnaire doit fournir l'adresse du ou des lieux proposés pour la réalisation des travaux ou la sauvegarde des documents.

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.

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 Biens ou services facultatifs, ou les deux

L'entrepreneur accorde au Canada l'option irrévocable d'acquérir les biens, les services ou les deux, qui sont décrits à Annexe A du contrat selon les mêmes conditions et aux prix et(ou) aux taux établis dans le 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.

L'autorité contractante peut exercer l'option à n'importe quel moment avant la date d'expiration du contrat en envoyant un avis écrit à l'entrepreneur.

1.2 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 (2013-03-21), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

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

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'un 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 ou de l'offrant devant avoir accès à des ren-seignements 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 ap-prouvée 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 pro-duction au niveau PROTÉGÉ tant que la DSCI, TPSGC ne lui en aura pas donné l'autori-sation 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 doi-vent PAS être attribués sans l'autorisation écrite préalable de la DSIC de TPSGC.

5. L'entrepreneur ou l'offrant 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);
b) le Manuel de la sécurité industrielle (dernière édition).

4. Durée du contrat

4.1 Période du contrat

La période du contrat est d'une durée de trois ans à partir de la date d'octroi du contrat.

4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus deux (2) période(s) supplémentaire(s) de une (1) 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 trente (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 six (6) 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 trente (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 des contrats
Travaux publics et Services gouvernementaux Canada
Direction générale des approvisionnements
Direction: Division des Services des Affaires et de Consultation

Adresse: 11 rue Laurier
Portage 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 lles Taxes applicables sont en sus.

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

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

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; et
b) une copie des factures, reçus, pièces justificatives pour tous les frais directs;

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 Conformité

Le respect des attestations et documentation connexe 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, à fournir la documentation connexe ou encore 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

A3050T (2010-01-11), Définition du contenu canadien
A3060C (2008-05-12), Attestation du contenu canadien

9. Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur en Ontario 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 (2013-03-21), 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
g) 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

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

ANNEXE A

ÉNONCÉ DES TRAVAUX

1.0 APERÇU

1.1 Introduction et historique

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

Même si le RG perçoit des remises dans le cadre de nombreux arrangements, les exigences décrites dans le présent Énoncé des travaux ne concernent que les services de transfert électronique de fonds (TEF) et ne visent à remplacer aucune autre forme de remises faites au RG, comme celles faites en espèces, par chèques, par cartes de crédit ou de débit, par débits préautorisés ou par paiements de factures en version papier ou électronique, pour lesquelles le RG a conclu des contrats et des arrangements distincts.

À l'heure actuelle, cinquante-quatre (54) ministères et organismes fédéraux, pour un total de quatre-vingt-huit (88) bureaux ministériels, acceptent les dépôts directs et les virements télégraphiques. Pour la période allant du 1er avril 2011 au 31 mars 2012, la valeur des paiements effectués par dépôt direct et par virement télégraphique s'est élevée à environ 2,4 G$ et 14,4 G$, respectivement.

Veuillez prendre note que certains virements télégraphiques entrants de grande valeur ont été exclus du présent arrangement. Par conséquent, les statistiques qui les concernent n'ont pas été intégrées aux estimations ni aux volumes fournis. Les transactions visées sont les transferts mensuels entre l'Office d'investissement du régime de pensions du Canada et Ressources humaines et Développement des compétences Canada.

1.2 Objectif

Le RG cherche à conclure un contrat officiel avec un seul fournisseur de services, ci-après appelé l'entrepreneur, pour le traitement des transferts électroniques de fonds (TEF) entrants. Le service doit couvrir les paiements libellés en dollars canadiens effectués au gouvernement par dépôt direct et par virement télégraphique.

1.3 Définitions

Veuillez vous reporter à l'*Annexe A, Appendice 1 – Définitions* pour consulter les définitions des termes utilisés dans le présent document.

1.4 Contrats actuels

À l'heure actuelle, le RG reçoit les fonds versés par dépôt direct et par virement télégraphique en vertu d'un contrat établi avec une seule institution financière canadienne.

1.5 Renseignements statistiques

L'*Annexe A, Appendice 6 – TEF rétrospectifs et prévus* présente les statistiques sur la valeur et le volume rétrospectifs des remises par dépôt direct et par virement télégraphique.

En outre, les prévisions relatives à la valeur et au volume font l'objet de l'*Annexe A, Appendice 7 – Valeurs et volumes prévus des remises pour 2014 à 2018*. 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 TEF.

2.0 EXIGENCES DÉTAILLÉES EN MATIÈRE DE SERVICES

2.1 Exigences opérationnelles générales

L'entrepreneur DOIT fournir les services suivants :

i. accepter les dépôts directs et les virements télégraphiques effectués en dollars canadiens à l'intérieur et à l'extérieur du Canada;

ii. veiller à ce que les transactions « propres », c'est-à-dire les transactions dans le cadre desquelles l'institution financière du client et l'entrepreneur représentent la même institution) soient traitées conformément aux règles de l'Association canadienne des paiements (ACP) concernant les dépôt directs et les virements télégraphiques (Règle F pour les dépôts directs et Règles du STPGV pour les virements télégraphiques) même si l'entrepreneur n'est pas techniquement assujetti à ces règles. L'objectif est de garantir que le traitement des transactions reste le même peu importe l'institution financière choisie par le client pour lancer la transaction;

iii. transférer le jour même au compte du RG ouvert à la Banque du Canada les fonds reçus avant 14 h HAE, conformément aux dispositions de la section 2.8 – Règlement. Tous les fonds reçus après 14 h HAE DOIVENT être transférées le jour ouvrable suivant;

iv. déclarer les renseignements sur les remises, au moyen d'un outil de rapports en ligne, aux bureaux ministériels compétents et au RG, conformément aux dispositions de la section 3.2 – Rapports en ligne;

v. fournir des rapports électroniques au RG sur les mouvements de compte (relevé bancaire) le jour ouvrable suivant, conformément à la section 3.1 – Rapports destinés au receveur général du Canada;

vi. répondre aux demandes de renseignements du RG concernant les transactions de TEF, conformément aux dispositions de la section 2.10 – Suivis et demandes de renseignements.

2.2 Ouverture d'un compte central

L'entrepreneur DOIT ouvrir, au Canada, un compte central du nom de « Receveur général du Canada – Remises de TEF ».

2.3 Ouverture de comptes auxiliaires

L'entrepreneur doit ouvrir un compte auxiliaire pour chaque bureau ministériel afin de faciliter l'établissement des rapports, conformément à la section 3.0 – Exigences en matière de rapports. Le solde des comptes auxiliaires DOIT être versé tous les jours dans le compte central. Autrement dit, la date de

présentation (date à laquelle l'entrepreneur reçoit les fonds) doit toujours être identique à la date de dépôt dans le compte central, sauf en cas de circonstances exceptionnelles.

2.4 Enregistrement des TEF dans le compte central et les comptes auxiliaires

i. L'entrepreneur DOIT enregistrer chacune des remises par TEF dans le compte auxiliaire pertinent dans l'heure qui suit leur réception.

ii. Chaque jour, l'entrepreneur doit verser le solde de chaque compte auxiliaire dans le compte central, la date de dépôt dans le compte central devant correspondre à la date de présentation de chaque transaction. Autrement dit, peu importe si les fonds sont transférés le jour même ou le lendemain à la Banque du Canada, la date de présentation et la date de dépôt dans le compte central doivent être identiques.

iii. Le RG attribuera un numéro d'autorisation unique à chaque bureau ministériel désirant profiter du service de TEF. L'entrepreneur DOIT indiquer ce numéro d'autorisation dans le relevé bancaire électronique pour chaque enregistrement de compte (autre que le transfert à la Banque du Canada). De plus, l'entrepreneur est incité à fournir un numéro de référence unique de TEF dans le relevé bancaire électronique pour chaque enregistrement de compte qui fait aussi partie des renseignements sur la remise déclarés au ministère concerné pour faciliter le rapprochement.

2.5 Rajustements demandés par l'entrepreneur

L'entrepreneur DOIT entrer chaque rajustement séparément dans le compte auxiliaire approprié. L'écriture initiale erronée DOIT être annulée, et l'écriture exacte DOIT être effectuée. L'entrepreneur DOIT, le jour même de l'enregistrement de compte, transmettre les pièces confirmant le rajustement au RG et au bureau ministériel concerné.

2.6 Conseils à l'égard des directives du remettant

L'entrepreneur DOIT prodiguer des conseils quant à l'élaboration de directives pour le remettant de TEF qui faciliteront la déclaration complète et exacte des renseignements sur la remise qu'exige le bureau ministériel en vue de déterminer le payeur, le bureau ministériel bénéficiaire et l'objet du paiement. Les directives doivent clairement indiquer le message qui doit accompagner chacune des transactions de sorte à ce que tous les frais bancaires imputés au bénéficiaire et à l'institution intermédiaire soient absorbés par le payeur. Les directives doivent en outre comprendre les renseignements dont le payeur a besoin pour lancer les transactions à l'intérieur et à l'extérieur du Canada.

2.7 Frais

Conformément à la section 2.6, les directives du remettant indiqueront que tous les frais bancaires imputés au bénéficiaire et à l'institution intermédiaire seront pris en charge par le payeur. Par conséquent, l'entrepreneur ne doit appliquer aucuns frais de TEF au montant initial du paiement.

2.8 Règlement

L'entrepreneur DOIT transférer le jour même de leur réception, au compte du RG ouvert auprès de la Banque du Canada, les fonds reçus avant 14 h HAE. Les fonds reçus après 14 h HAE DOIVENT être transférés au compte du RG ouvert auprès de la Banque du Canada le jour ouvrable suivant.

Le jour où les fonds sont transférés à la Banque du Canada correspond à la « date de règlement ». Les intérêts sur le fonds de caisse s'appliquant aux transferts réalisés le jour suivant seront calculés conformément aux dispositions de la section 2.9 – Flottants.

Avant 15 h HAE, l'entrepreneur doit établir et envoyer à la Banque du Canada un message MT103 concernant un paiement du STPGV destiné au RG. Ce message doit faire état des soldes du jour même relatifs à tous les fonds reçus avant 14 h HAE, de même que des soldes non réglés de la veille. La mise en forme requise à l'égard du message MT103 est indiquée à l'*Annexe A, Appendice 5 – Exigences de la Banque du Canada en matière de formatage en ce qui a trait au STPGV*. Veuillez noter que les soldes du jour même et de la veille doivent faire l'objet de messages MT103 distincts.

2.9 Flottants

L'entrepreneur DOIT verser au RG des intérêts flottants pour tous les fonds dont la date de règlement est postérieure à la date de présentation. Le montant de ces intérêts 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 %); il est toutefois sujet à changement.

En cas d'erreur de la part du RG ou de l'entrepreneur, ou de circonstances exceptionnelles ayant une incidence négative sur les flottants en sus du taux d'intérêt précisé dans le protocole d'entente pour le RG ou pour l'entrepreneur, un taux d'intérêt supérieur peut être versé, jusqu'à concurrence des pertes financières réelles subies. Une telle situation DOIT être examinée par le RG.

2.10 Suivis et demandes de renseignements

L'entrepreneur DOIT tout mettre en œuvre pour répondre à toute demande de renseignements ou d'éclaircissements sur les remises adressée par le RG dans un délai de cinq (5) jours ouvrables. S'il n'a pas obtenu de réponse dans les délais prescrits, le RG peut acheminer la demande à un échelon supérieur de l'organisation de l'entrepreneur. Les demandes de suivi et les demandes de renseignements du RG porteront un numéro d'enquête, lequel DOIT être indiqué dans toutes les réponses.

3.0 EXIGENCES EN MATIÈRE DE RAPPORTS

3.1 Rapports destinés au receveur général du Canada

L'entrepreneur DOIT fournir au RG un relevé bancaire électronique quotidien (EDI 821) concernant le compte central avant 8 h HAE le premier jour ouvrable suivant la date du dépôt dans le compte central. Dans le relevé bancaire EDI 821, l'entrepreneur doit :

i. déclarer chacune des transactions de virement télégraphique et de dépôt direct séparément;

ii. déclarer chacun des rajustements séparément sur le relevé bancaire EDI 821;

iii. s'assurer que le numéro d'autorisation du RG attribué au compte auxiliaire figure dans le segment REF 02;

iv. veiller à ce que les bons codes de transaction financière associés à chacun des dépôts directs entrants, des virements télégraphiques entrants et des rajustements soient indiqués dans le segment FIR01. Nous n'exigeons pas que les transferts réalisés entre les comptes auxiliaires et le compte central, et entre le compte central et la Banque du Canada soient inscrits dans le relevé bancaire EDI 821. Toutefois, si l'entrepreneur souhaitait tout de même le faire, il devra affecter des codes de transaction distincts à ces types de transfert dans le segment FIR01 afin de nous permettre de distinguer les transactions réelles des mouvements de fonds;

v. s'assurer que la date à laquelle les fonds ont été déposés dans le compte central (date de dépôt dans le compte central) est inscrite dans le segment BGN03;

vi. s’assurer que la date à laquelle l’entrepreneur a reçu chacune des transactions (date de présentation) figure dans le segment FIR07.

Le protocole actuel et la mise en correspondance des relevés bancaires électroniques sont fournis aux *appendices 2, 3 et 4 de l'Annexe A*.

3.2 Rapports en ligne

L’entrepreneur DOIT fournir un accès en ligne protégé en mode « lecture seule » à toutes les activités de compte, y compris aux dépôts directs, aux virements télégraphiques, aux rajustements, ainsi qu’aux transferts au compte central et à la Banque du Canada. Chaque bureau ministériel ne doit avoir accès qu’aux transactions qui portent son numéro d’autorisation, tandis que des droits généraux doivent être accordés au RG de sorte à ce qu’il puisse visionner les transactions associées à tous les numéros d’autorisation, ainsi que les activités liées au compte central. L'entrepreneur doit fournir les services suivants à l'égard des rapports en ligne :

i. faire en sorte que les renseignements sur les dépôts directs et les virements télégraphiques soient disponibles dans l’heure qui suit leur réception par l’entrepreneur. Dans certains cas, sur demande du RG, l’entrepreneur devra également fournir au RG et au bureau ministériel compétent des rapports en temps réel sur des transactions précises sensibles au temps;

ii. limiter l'accès aux employés autorisés des bureaux ministériels qui bénéficient d'un accès en « lecture seule »;

iii. veiller à ce que les données soient accessibles dans l’outil de rapports en ligne pendant au moins six (6) mois;

iv. avoir la capacité de permettre aux ministères de télécharger les données vers leurs propres systèmes à l'aide d'un tableur électronique;

v. offrir un service d’assistance bilingue, conformément aux dispositions de la section 5.2 – Centre d’assistance, aux fins de l’établissement des comptes des nouveaux utilisateurs et de la résolution de problèmes;

vi. à l’égard des rajustements, rendre disponibles dans l’outil de rapports en ligne le motif des rajustements effectués;

vii. à l’égard des virements télégraphiques, rendre disponibles dans l’outil de rapports en ligne les renseignements sur les remises figurant dans le message de paiement qu’il a reçu;

viii. à l’égard des dépôts directs, à tout le moins communiquer les renseignements sur les remises suivants qui figurent dans le type d’enregistrement logique « C » établi conformément à la Norme 005 de l’ACP (si le remettant le reçoit) :

   a. le nom abrégé de l'émetteur (élément de données 11) ou, si possible, le nom au long de l'émetteur (élément de données 13);
   b. le type de transaction (élément de données 04);
   c. les renseignements divers de l'émetteur (élément de données 18);
   d. le montant (élément de données 05).

4.0 ÉLABORATION ET MISE EN ŒUVRE DU SERVICE DE REMISE DES TEF

4.1 Mise en œuvre du service

Les travaux de mise en œuvre doivent commencer dans les cinq (5) jours ouvrables suivant la date d'attribution du contrat. En outre, l'entrepreneur doit :

i. dans les deux (2) semaines suivant l'attribution du contrat (à moins d'une entente contraire), informer le RG à propos du service de remise, y compris des pratiques exemplaires, et répondre à toutes ses questions;

ii. dans les deux (2) semaines suivant l'attribution du contrat, passer en revue les formulaires d'établissement du service de TEF et cerner les autres renseignements dont il a besoin;

iii. dans les deux (2) semaines suivant l'attribution du contrat, fournir 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 traiter les questions liées à l'administration du contrat, de même que celles des personnes-ressources de deuxième et troisième niveaux, et communiquer les délais d'exécution maximaux auxquels on peut s'attendre. Les coordonnées du personnel autorisé présentées par l'entrepreneur doivent comprendre celles des personnes-ressources responsables des activités quotidiennes, des questions de sécurité d'accès, du soutien informatique et technique pour la période de transition et les activités courantes, ainsi que de l'envoi de la facturation mensuelle du RG pour les services rendus;

iv. dans les deux (2) mois suivant l'attribution du contrat (à moins d'une entente contraire), mettre en œuvre les bureaux ministériels existants qui profitent du service de TEF;

v. se conformer à la configuration électronique et aux exigences de mise à l'essai prévues à l'*Annexe A, Appendice 2 – Protocole actuel de déclaration électronique des relevés bancaires*;

vi. être disponible aux fins de la mise à l'essai des fichiers et des rapports électroniques dans un environnement d'essai;

vii. faire passer la transmission électronique à l'environnement de production, une fois l'approbation du RG reçue;

viii. communiquer avec la Banque du Canada afin de mettre la dernière main aux ententes de règlement;

ix. respecter toute autre exigence énoncée dans l'Énoncé des travaux;

x. être tout à fait opérationnel en ce qui concerne les services de TEF décrits dans le présent Énoncé des travaux au plus tard deux (2) mois après la date d'attribution du contrat, à moins d'entente contraire conclue avec le RG.

4.2 Mise en œuvre de nouveaux bureaux ministériels

Au besoin, et seulement sur réception d'un formulaire de demande de TEF autorisé, l'entrepreneur DOIT fournir des services de remise des TEF aux bureaux ministériels. Le formulaire, sujet à changement, est reproduit à l'*Annexe A, Appendice 8 – Formulaire de demande de TEF*.

Tout ajout ou suppression de service demandé par un ministère devra également être appuyé par un formulaire de demande de TEF autorisé.

Les ministères feront leur demande officielle d'établissement ou de modification d'un bureau ministériel en transmettant un formulaire de demande de TEF au RG, qui l'acheminera ensuite à l'entrepreneur. Les parties concernées extrairont du formulaire les renseignements dont elles ont besoin et y indiqueront leur identificateur (p. ex. le numéro d'autorisation du RG, le numéro de compte central et le numéro de compte auxiliaire). Une fois tous les identificateurs reçus, le RG retournera le formulaire approuvé au ministère concerné.

Sur réception d'un formulaire de demande de TEF approuvé, l'entrepreneur DOIT :

i. en extraire tous les renseignements dont il a besoin;

ii. y inscrire tous les identificateurs nécessaires, tels que le numéro de compte auxiliaire;

iii. retourner le formulaire au RG dans les trois (3) jours ouvrables suivant sa réception;

iv. être disposé à mettre en œuvre les nouveaux services ou les services modifiés dans les deux (2) semaines suivant la réception du formulaire (à moins d'une entente écrite contraire);

v. fournir de l'assistance au besoin pour la mise à l'essai ou la mise en œuvre des services de TEF, nouveaux ou modifiés;

vi. fournir un soutien continu, au besoin, par exemple dans le cadre des essais relatifs aux nouveaux remettants associés à des transactions de grande valeur.

L'entrepreneur ne doit pas commencer le travail avant qu'un formulaire de demande de TEF n'ait été autorisé par le responsable du projet. L'entrepreneur reconnaît que tout travail effectué avant l'autorisation d'un formulaire de demande de TEF le sera à ses propres risques et frais.

4.3 Documentation et formation

L'entrepreneur DOIT fournir au RG et aux bureaux ministériels une documentation bilingue, complète et à jour (comme le guide de l'utilisateur) ainsi qu'une formation (comme le soutien continu d'un centre d'assistance) sur l'outil de rapports en ligne qu'il fournit.

Il incombera au RG d'élaborer les modalités d'engagement relatives au service de TEF. Ces modalités d'engagement comprendront notamment les éléments suivants :

- un aperçu du service de TEF;
- une description du processus lié aux dépôts directs et aux virements télégraphiques;
- une description du processus d'établissement des bureaux ministériels;
- des exemples de directives du remettant;
- des renseignements sur le service d'assistance pour l'établissement de comptes d'utilisateur mise en place et la résolution de problèmes.

L'entrepreneur DOIT aider le RG dans l'élaboration de ces modalités d'engagement, ce qui peut inclure la formulation de recommandations sur le guide et un examen de son contenu.

4.4 Dispositions concernant la 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 service à un volume réduit, selon les mêmes modalités et tarifs prévus au contrat, pendant une

période ne dépassant pas six (6) mois afin de régler toutes les transactions. La période totale du contrat comprend la phase opérationnelle, mais pas la 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 de transition, un fichier de données électronique contenant tous les renseignements recueillis pendant la période du contrat.

L'entrepreneur s'engage en outre à faciliter la transition vers tout entrepreneur subséquent à la fin de ce contrat, et ce, sans interruption de service et avec un minimum de perturbation des processus et des opérations du gouvernement.

5.0 AUTRES EXIGENCES

5.1 Transactions en devise

Le service est conçu exclusivement pour l'acceptation et le traitement des remises de TEF libellées en dollars canadiens. L'information transmise par les ministères aux remettants devra faire ressortir cette exigence. Dans le cas où des remises seraient effectuées en monnaie étrangère, l'entrepreneur DOIT rejeter ces opérations et en informer le RG.

5.2 Centre d’assistance

Un service d’assistance dans les deux langues officielles DOIT être fourni par l'entrepreneur tous les jours ouvrables, soit du lundi au vendredi, de 8 h 30 et 17 h HAE.

L'entrepreneur DOIT fournir un numéro de téléphone sans frais pour le centre d’assistance, en plus d'un service de courriel.

Pour aider le RG à rapprocher le compte central, l'entrepreneur DOIT fournir les numéros de téléphone des personnes qui collaboreront à la résolution des problèmes.

L’entrepreneur DOIT traiter directement avec les bureaux ministériels concernant tout problème technique à l’égard de l’outil de rapports en ligne.

5.3 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 sa pièce jointe 1 – Exigences en matière de sécurité de la TI*.

5.4 Plan d'urgence et de reprise après sinistre

Comme il est indiqué dans l'*Annexe C et sa pièce jointe 1 – Exigences en matière de la sécurité de la TI*, l'entrepreneur DOIT disposer d’un plan officiel d'urgence et de reprise après sinistre qu’il invoquera 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. En pareils cas, l'entrepreneur DOIT tout mettre en œuvre pour maintenir les communications et les rapports normaux avec le RG et les bureaux ministériels en utilisant d'autres moyens qui auront été convenus entre les parties.

5.5 Évaluation périodique de la menace et des risques

À la demande du responsable de projet, l'entrepreneur DOIT fournir les renseignements nécessaires pour aider le Canada à préparer un énoncé de sensibilité et une évaluation de la menace et des risques en rapport avec les services de TEF fournis.

5.6 Association canadienne des paiements

L'entrepreneur doit être un membre participant du Système de transfert de paiements de grande valeur (STPGV) de l'Association canadienne des paiements (ACP) et conserver son statut pendant la période d'exécution du contrat et toute période optionnelle de prolongation, y compris toute période de transition.

5.7 Langue

L'entrepreneur DOIT pouvoir fournir ses services dans les deux langues officielles du pays, soit le français et l'anglais. Le personnel responsable de la formation (centre d'assistance) DOIT fournir des services bilingues (en français et en anglais). Cependant, le matériel publicitaire et les documents traitant, entre autres, des modalités d'engagement, des règles et des règlements peuvent être en anglais et, si possible, en français.

Si le responsable de projet juge inacceptables les versions françaises disponibles, le RG se réserve le droit d'obtenir, à ses frais, des versions retraduites que seuls les bureaux ministériels pourront utiliser.

On peut consulter la *Loi sur les langues officielles* de même que les politiques et les publications du Secrétariat du Conseil du Trésor dans les sites Web suivants :
http://laws-lois.justice.gc.ca/fra/lois/O-3.01/
http://www.tbs-sct.gc.ca/pol/index-fra.aspx

5.8 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, le code SWIFT et le STPGV) par la norme ISO 20022. Le RG souhaite ainsi être l'un des premiers à adopter cette nouvelle norme. Si la norme ISO 20022 devait être mise en œuvre pendant la période visée par le présent contrat, l'entrepreneur DEVRA, à la demande du RG, accepter et envoyer les fichiers de transfert automatisé de fonds, les fichiers de code SWIFT et les fichiers du STPGV dans ce nouveau format.

Si, comme étape intermédiaire à l'adoption de la norme ISO 20022 ou en remplacement de cette dernière, l'ACP décidait de mettre à jour la Norme 005 afin de faciliter la transmission de données améliorées sur les remises, l'entrepreneur DEVRA également se conformer à cette nouvelle norme.

5.9 Futurs besoins opérationnels

La manière dont le RG fait des affaires est susceptible de changer avec le temps, au fil de l'élaboration de nouveaux modes de prestation et de l'amélioration des technologies. Le secteur des services financiers procède à des changements similaires, comme l'intégration de nouveaux services de perception qui sont plus rapides, plus économiques et plus pratiques que par le passé. C'est en réponse aux demandes du grand public que sont proposés ces services, et les attentes de la clientèle sont grandissantes, car elle est au fait des possibilités qu'offre la technologie.

Le responsable de projet peut demander à l'entrepreneur de présenter des solutions novatrices en matière de technologies et de services pendant la période du contrat et les années d'option, en vue d'améliorer le service à la clientèle et de réduire les coûts. Inversement, l'entrepreneur peut également suggérer au responsable de projet d'adopter de telles solutions.

Tout nouveau service de ce type qui sera approuvé ne sera mis en œuvre que si l'on ajoute au contrat une modification approuvée et officielle. Le RG ne renonce pas à son droit de demander une soumission concurrentielle pour les nouveaux services. Ces nouveaux services peuvent inclure, sans s'y limiter, ce qui suit :

- des services pour accepter et traiter d'autres types de remises par TEF;
- des nouvelles technologies pour les services de TEF ainsi que de nouvelles méthodes de déclaration des remises;
- des services pour normaliser les processus dans l’ensemble des ministères fédéraux ou pour apporter des modifications qui réduiraient les coûts et amélioreraient l'efficience ainsi que la qualité des services offerts.

ANNEXE A, APPENDICE 1
DÉFINITIONS

Les définitions suivantes s'appliquent au présent Énoncé des travaux et peuvent avoir un sens différent dans d'autres contextes.

Bureau ministériel	Bureau ministériel fédéral qui a été établi par le RG et autorisé par celui-ci à accepter les remises de TEF. Aussi appelé « bénéficiaire ». Un bureau ministériel peut viser un ministère fédéral, ou encore une division ou un programme précis au sein d'un ministère.
Client et remettant	Personne ou organisation qui effectue des remises de TEF aux bureaux ministériels.
Compte central	Compte établi au nom de « Receveur général du Canada – Remises de TEF », spécialement créé pour le dépôt des remises de TEF du gouvernement.
Comptes auxiliaires	Comptes établis au nom du receveur général dont le solde passe quotidiennement dans le compte central. Grâce aux comptes auxiliaires, il est possible d'associer chaque transaction au bureau ministériel pertinent.
Date de dépôt dans le compte central	Date à laquelle le RG reçoit des valeurs dans le compte central.
Date de présentation	Date à laquelle l'entrepreneur reçoit une transaction de dépôt direct ou de virement télégraphique.
Date de règlement	Date à laquelle le RG reçoit des valeurs à la Banque du Canada.
Dépôt direct	Dépôt de fonds directement dans un compte bancaire comme mode de paiement. Le dépôt direct est généralement utilisé pour la paye et les remboursements d'impôt.
Fonds de caisse	Valeur des rentrées de fonds du gouvernement du Canada qui sont en circulation entre l'entrepreneur et la Banque du Canada.
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 d'autorisation	Nombre composé de huit chiffres attribué par le RG à un bureau ministériel qui a été autorisé à accepter les remises de TEF.
Payeur	Personne ou organisation à l'origine d'une transaction de dépôt direct ou de virement télégraphique.
STPGV	Système de transfert de paiements en temps réel appartenant à l'Association canadienne des paiements et exploité par celle-ci qui sert au traitement de paiements de grande valeur et au transfert électronique de messages de paiement entre membres participants du Système de traitement de paiements de grande valeur (STPGV).
TEF	Transfert électronique de fonds, lequel comprend les remises au titre des dépôts directs et des virements télégraphiques.
Valeur jour suivant	Lorsque la date de règlement correspond au jour ouvrable suivant la date de présentation.
Valeur même jour	Lorsque la date de règlement est la même que la date de présentation.

ANNEXE A, APPENDICE 2

Protocole actuel pour les rapports électroniques sur les relevés bancaires

Le protocole actuel pour les rapports électroniques sur les relevés bancaires est le format standard EDI ANSI X12, à savoir :

1. Ensembles d'opérations

Les parties s'échangent les ensembles d'opérations EDI suivants:

a. Caractéristiques de l'enveloppe ANSI X12 (l'" enveloppe ");
b. Rapports d'information financière ANSI X12 821 (les " 821 "); et
c. Accusé de réception fonctionnel ANSI X1 2 997 (le " 997 ").

L'enveloppe et les rapports 821 sont reproduits ci-joint dans l'appendice 3 et l'appendice 4 de l'annexe A.

2. Données pour les rapports 821

l'heure actuelle, les rapports 821 doivent comprendre les données suivantes:

a. Numéro de l'institution financière attribué par l'Association canadienne des paiements;
b. Numéro de transit de la succursale auprès de laquelle le compte est ouvert;
c. Le numéro du compte faisant l'objet du rapport;
d. Le code de l'opération (type) :

i. On doit au moins indiquer des codes distincts pour les opérations autorisées, soit :
   - les dépôts directs;
   - les rajustements bancaires relatifs aux dépôts directs;
   - les virements télégraphiques;
   - les rajustements bancaires relatifs à des virements télégraphiques;
   - les opérations relatives à des virements à la Banque du Canada ou entre les sous-comptes et le compte concentrateur.

ii. Écritures non autorisées:

Il FAUDRA prendre des mesures pour mettre un terme aux écritures non autorisées. Bien que les types d'opérations suivants ne soient pas autorisés pour le présent Énoncé des travaux, il faudra indiquer au minimum des codes distincts, si on doit traiter ces opérations, pour ce qui est:

- les dépôts manuels au comptoir;
- les rajustements bancaires relatifs aux dépôts manuels au comptoir;
- les effets retournés correspondant aux dépôts manuels au comptoir;
- les dépôts électroniques par carte;
- les rajustements bancaires relatifs aux dépôts électroniques par carte;
- les effets retournés relativement aux dépôts électroniques par carte;
- les dépôts effectués par EDI à l'aide du formulaire 820/823;
- les rajustements bancaires relatifs aux dépôts effectués par EDI à l'aide du formulaire 820/823;
- les effets retournés relatifs aux dépôts effectués par EDI à l'aide du formulaire 820/823 (dans les cas autorisés);
- les dépôts effectués par débits préautorisés (DPA);
- les rajustements bancaires relatifs aux dépôts effectués par débits préautorisés (DPA);
- les effets retournés relatifs aux dépôts effectués par débits préautorisés (DPA).

e. Date de concentration des opérations;
f. Montant des opérations;
g. Numéros de référence RR, ZZ, PQ, IT, IX, VR et DE précisés dans l'appendice 4 de l'annexe A.

3. Configuration et période d'essai

À l'heure actuelle, le receveur général exige que les entrepreneurs :

a. fournissent, au moins six (6) semaines avant la date de la mise en œuvre, tous les renseignements sur les boîtes postales et tous les autres renseignements pertinents pour la configuration du système.
b. déposent, au moins six (6) semaines avant la date de la mise en œuvre, la liste des codes mnémoniques (avec leur signification) à utiliser comme codes d'opération types.
c. transmettent, dans la boîte postale d'essai du receveur général:

    i. les données d'essai générales 821 (qui auront été compilées et acceptées par le receveur général) au moins quatre (4) semaines avant la date de la mise en œuvre, et selon la demande du receveur général par la suite;

    ii. les données réelles (en dollars) 821 pour le compte, chaque jour, à partir d'au moins trois (3) semaines avant la date de la mise en œuvre et selon la demande du receveur général par la suite.

4. Processus d'établissement des rapports au moment de la mise en œuvre

À l'heure actuelle, le receveur général exige que les entrepreneurs :

a. respectent le plan d'essai et les procédures d'autorisation du receveur général, sauf convention contraire. Ces plans et ces procédures seront fournis sur demande.
b. transmettent chaque jour ouvrable, en texte clair, un relevé 821 du Compte dans la boîte postale de production électronique du receveur général au plus tard à 8h heure normale de l'est (HNE) le premier jour ouvrable suivant la date de concentration.
c. acceptent les opérations positives ou négative 997 du receveur général pour donner suite à chaque relevé 821 transmis par l'entrepreneur, en prenant des mesures complémentaires si ce dernier ne reçoit pas une opération 997 après chaque transmission. Il faut prendre des mesures complémentaires au plus tard à heure normale de l'est (HNE) le jour même de chaque transmission 821. Ces mesures DOIVENT consister en un appel téléphonique à passer au receveur général.
d. corrigent le relevé 821 et le retransmettent dans un délai de deux heures suivant sa réception, après avoir reçu une opération négative 997 (ISA09 et ISA10 de l'enveloppe ANSI X1 2).
e. si on ne peut pas établir les rapports selon les modalités ci-dessus, et à la demande du receveur général, fournissent au lieu d'un relevé 821, un exemplaire imprimé ou une copie électronique des données énumérées dans la section 2 de l'appendice 2 de l'Annexe A. Il FAUDRA s'entendre sur le choix du support.
f. transmettent, chaque jour ouvrable, au receveur général, un exemplaire des pièces justificatives pour toutes les écritures passées dans le compte et ne faisant pas l'objet de cet énoncé des travaux, pour qu'il parvienne au receveur général le même jour que le relevé 821.

5. L'expéditeur assume les coûts de transmission

Le receveur général demande aux entrepreneurs d'assumer tous les coûts liés à la transmission des relevés 821. Cette mesure vise également les envois en provenance et à destination de la boîte de réception du receveur général.

Annexe A, Appendice 3

Spécifications de l'enveloppe 821/152

VERSION 003010

Receveur général

Édition 3.02

Spécifications de l'enveloppe du Receveur général

Numéro de version du contrôle de l'échange 00200

ID DU SEG.	Nom	Requis	Boucle
ISA	Segment en-tête du contrôle de l'échange	O	1
GS	Segment en-tête du groupe fonctionnel	O	GS 1 > 1
GE	Segment fin du groupe fonctionnel	O	GE 1 > 1
IEA	Segment fin du contrôle de l'échange	O	1

***(O = Obligatoire*)**

Note : Dans cette édition 3.02 les segments “GS01 & GS08” ont été modifiés.

ISA

Segment en-tête du contrôle de l'échange

Indique le début de l'échange

ISA	**ISA01 I01**	*	**ISA02 I02**	*	**ISA03 I03**	*	**ISA04 I04**	*	**ISA05 I05**	
*	Qual. de l'inform. sur l'autorisation		Information sur l'autorisation		Qual. de l'information sur la sécurité		Information sur la sécurité		Qual. de l'ID de l'échange	
	O ID 2/2		**O AN 10/10**		**O ID 2/2**		**O AN 10/10**		**O ID 2/2**	

	ISA06 I06	*	**ISA07 I05**	*	**ISA08 I07**	*	**ISA09 I08**	*	**ISA10 I09**	
*	ID de l'envoyeur de l'échange		Qual. de l'ID de l'échange		ID du destinataire de l'échange		Date de l'échange		Heure de l'échange	
	O AN 15/15		**O ID 2/2**		**O AN 15/15**		**O DT 6/6**		**O TM 4/4**	

	ISA11 I10	*	**ISA12 I11**	*	**ISA13 I12**	*	**ISA14 I13**	*	**ISA15 I14**	
*	Id du contrôle de l'échange		No. de version de l'échange		No. de contrôle de l'échange.		Accusé de réception demandé		Indicateur d'essais	
	O ID 1/1		**O ID 5/5**		**O N0 9/9**		**O ID 1/1**		**O ID 1/1**	

	ISA16 I15		
*	Séparateur de sous-éléments	N / L	
	O AN 1/1		

ISA01 Qualificatif de l'information sur l'autorisation
Code qui identifie le type de l'information dans le segment ISA02. Employer "00" pour indiquer l'absence d'information sur l'autorisation.

ISA02 Information sur l'autorisation
Employé pour une identification ou une autorisation additionnelle de l'envoyeur ou des données contenues dans l'échange. Inutilisé.

ISA03 Qualificatif de l'information sur la sécurité
Code qui identifie le type de l'information du segment ISA04. Employez "00" pour indiquer l'absence d'information sur la sécurité.

ISA04 Information sur la sécurité
Identifie l'information, en matière de sécurité, relative à l'envoyeur ou aux données de l'échange. Inutilisé.

ISA05 Qualificatif de l'ID de l'échange
Désigne la structure de codage employée pour identifier l'envoyeur. Défini par l'en-voyeur. Par exemple, utilisé "12" pour un numéro de téléphone ou "01" pour un numé-ro "DUNS".

ISA06 ID de l'envoyeur de l'échange
Identification publiée de l'envoyeur. Définie par l'envoyeur.

ISA07 Qualificatif de l'ID de l'échange
Désigne la structure de codage adoptée pour identifier le destinataire.
Employer "12" pour numéro de téléphone ou "01" pour un numéro "DUNS".

ISA08 ID du destinataire de l'échange
Doit être fournie par le Receveur général (RG), conformément au plan d'essai et pro-cédures de passge à la production du Receveur général.

ISA09 Date de l'échange
Date de création de l'échange. Le format doit être : "AAMMJJ".

ISA10 Heure de l'échange
Heure de création de l'échange. Le format doit être : "HHMM".

ISA11 ID de contrôle de l'échange
Code désignant l'organisme de normalisation. Employer "U".

ISA12 Numéro de version de l'échange
Numéro de version des segments du contrôle de l'échange. Employer "00200".

ISA13 Numéro de contrôle de l'échange
Identification exclusive de l'échange. Créée par l'envoyeur et doit être identique à cel-le indiquée dans le segment IEA02.

ISA14 Accusé de réception demandé
Code indiquant si l'envoyeur a demandé, ou non, un accusé de réception. Le Receveur général ne tiendra pas compte de cette information.

ISA15 Indicateur d'essais
Code indiquant si l'échange contient des données d'essais ou de production.
Employer soit "P" pour production, soit "T" pour essai.

ISA16 Séparateur de sous-éléments.
Caractère de séparation des sous-groupes d'éléments de données.
Le Receveur général ne tiendra pas compte de cette information.

GS

Segment en-tête du groupe fonctionnel

Indique le début d'un groupe fonctionnel de documents.

GS	**GS01 479**		**GS02 142**		**GS03 124**		**GS04 29**		**GS05 30**	
*	Code d'ID fonctionnel	*	Code de l'envoyeur de l'application	*	Code du destinataire de l'application	*	Date	*	Heure	
	O ID 2/2		**O AN 2/12**		**O AN 2/12**		**O DT 6/6**		**O TM 4/4**	

	GS06 28		**GS07 455**		**GS08 480**	
*	Numéro de contrôle du groupe	*	Code de l'organisme responsable	*	Code d'ID de la version/édition	N / L
	O N0 1/9		**O ID 1/2**		**O AN 1/12**	

GS01 Code d'identification fonctionnel
Code qui identifie un groupe de documents informatisés relatifs à une application.
Documents informatisés et codes acceptables pour le RG :

Document informatisé	Code
821	FR
152	GR
820	RA
823	LB

GS02 Code de l'envoyeur de l'application
Code qui identifie l'envoyeur du groupe fonctionnel.

GS03 Code du destinataire de l'application
Code qui identifie le destinataire du groupe fonctionnel. Employer "RECGEN".

GS04 Date
Date de création du groupe. Le format doit être : "AAMMJJ".

GS05 Heure
Heure de création du groupe. Le format doit être : "HHMM".

GS06 Numéro de contrôle du groupe
Identification exclusive du groupe. Créée par l'envoyeur et doit être identique à la valeur indiquée dans GE02.

GS07 Code de l'organisme responsable
Code qui identifie l'organisme de normalisation adopté pour le groupe. La valeur doit être "X".

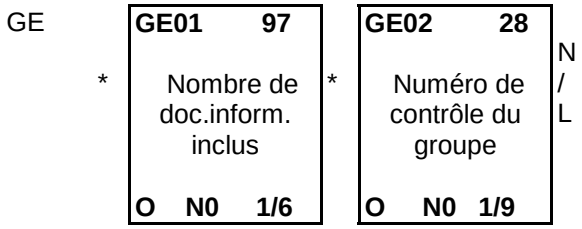
GS08 Numéro d'édition de la version
Versions normalisées du Receveur général. Des versions ultérieures peuvent être adoptées, moyennant entente avec l'industrie.

Document informatisé	Version
821, 820	“003010”
152, 823, 820	“003030”

GE

Segment fin du groupe fonctionnel

Indique la fin d'un groupe fonctionnel de documents



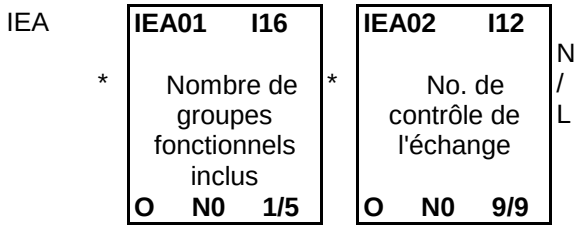
GE01 Nombre de documents informatisés
La valeur doit être identique au nombre de documents informatisés inclus dans le groupe fonctionnel.

GE02 Numéro de contrôle du groupe
Doit être identique à la valeur de GS06.

IEA

Segment fin du contrôle de l'échange

Indique la fin de l'échange



IEA01 Nombre de groupes fonctionnels
La valeur doit être identique au nombre de groupes fonctionnels contenus dans l'échange.

IEA02 Numéro de contrôle de l'échange
Identification exclusive de l'échange. Doit être identique à la valeur de ISA13.

ANNEXE A, APPENDICE 4

821 ÉTAT DE COMPTE

VERSION 003010

(Rapport de l'information financière du Receveur général)

Édition 2.12

Rapport de l'information financière 821 (X.12 version 3010)
Receveur Général du Canada (édition 2.12)

Moyennant entente avec le secteur privé, le receveur général (RG) établira et fournira des documents de mappage des données pour les versions postérieures à la version 3010.

Table 1

ID DE SEG.	Nom	Exig. ANSI	Max.	Exig. R.G.	Min.	Max.	Boucle
ST	En-tête du document informatisé	O	1	O	1	1	
BGN	Segment en-tête	O	1	O	1	1	
N1	Nom (expéditeur de l'information)	O	1	O	1	1	**N1/1**
PER	Contact pour les communications administratives	F	>1	F		>1	
N1	Nom (destinataire de l'information)	O	1	O	1	1	**N1/>1**
PER	Contact pour les communications administratives	F	>1	F		>1	
ACT	Identification du compte	F	1	O	1	1	**ACT/1**
CUR	Monnaie	F	1	F		1	
BAL	Détails du solde	F	>1	O	1	>1	
FIR	Information financière	F	1	F	1	1	**FIR/>1**
REF	Numéros de référence	F	>1	C	0	2	
SE	Fin du document informatisé	O	1	O	1	1	

(O = obligatoire; F = facultatif; C = conditionnel)

Notes :

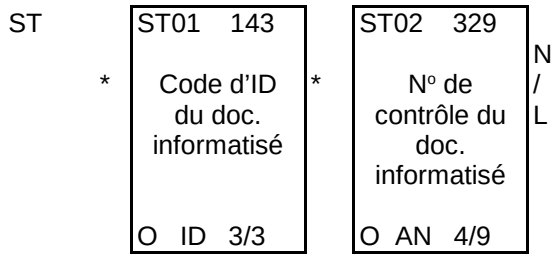
1. N1 (première occurrence privilégiée) est l'expéditeur du 821

2. N1 (deuxième occurrence privilégiée) est le destinataire du 821 (le receveur général)

Segments et données

ST
En-tête du document informatisé

Il s'agit du début du document informatisé.

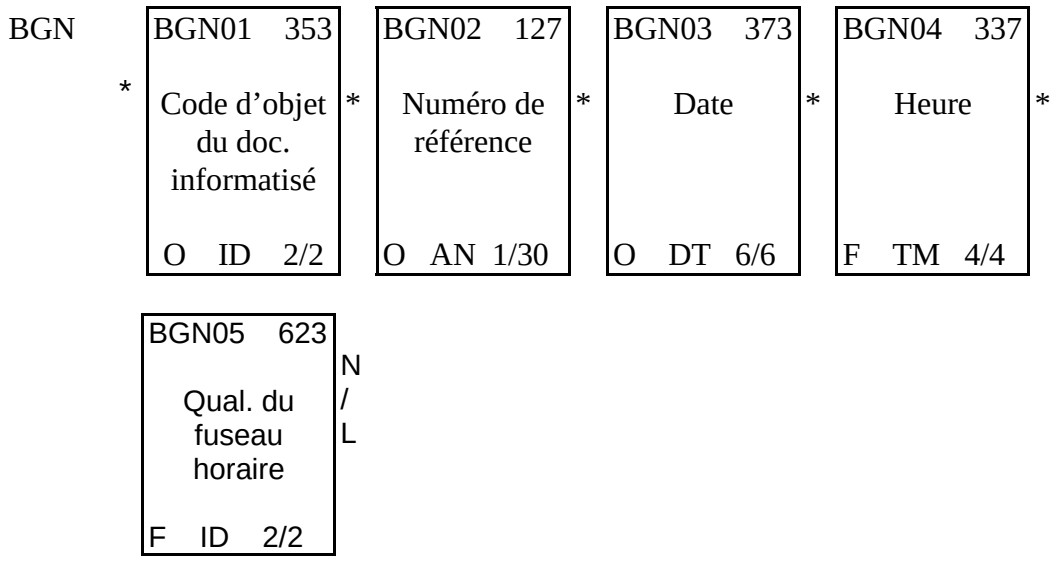


ST01 - Code du document informatisé
Élément obligatoire portant la valeur " 821 "

ST02 - Numéro de contrôle du document informatisé
Ce numéro de contrôle désigne de façon exclusive chaque document échangé entre des partenaires commerciaux. On suggère d'augmenter ce numéro de un pour chaque document informatisé suivant.

BGN
Segment en-tête

Il s'agit du début du document informatisé.



BGN01 Code désignant l'objet du document informatisé.
Élément obligatoire portant la valeur " 00 " (retenues, acomptes provisionnels ou arriérés d'impôt sur le revenu) ou la valeur " 22 " (tous les autres états de compte).
Obligatoire. Élément de la norme EDI mais inutilisé par le RG.

BGN02 Code désignant de façon exclusive le document informatisé.
Ce numéro se compose de deux éléments :

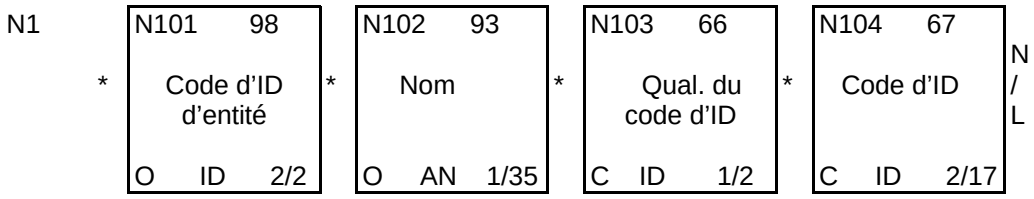
1. le code de quatre chiffres de l'institution financière (IF) membre de l'ACP et indiquant l'IF d'origine;
2. une combinaison d'au plus 26 chiffres, lettres et/ou espaces désignant exclusivement l'opération.

BGN03 Code désignant la date du jour ouvré à laquelle on a noté le solde du compte. (AAMMJJ)

BGN04 BGN05
Codes inutilisés.

N1
NOM (première occurrence privilégiée)

La première occurrence du segment N1 identifie l'envoyeur de l'information financière.



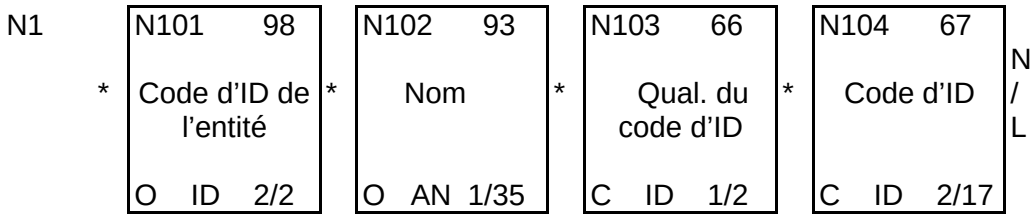
N101 - Code d'identification de l'entité
Élément obligatoire portant la valeur " FW " et désignant l'expéditeur

N102 - Nom
Nom de l'IF qui envoie l'information

N103 - N104
Codes inutilisés

N1
NOM (deuxième occurrence privilégiée)

La deuxième occurrence du segment N1 désigne le destinataire de l'information financière.



N101 - Code d'identification de l'entité
Élément obligatoire avec la valeur " AQ " et désignant le " compte de (la partie destinataire) "

N102 - Nom

« REC GEN » « Receveur général du Canada »	Opérations dans les comptes de dépôt, versements électroniques de l'ADRC.
« 205 REC GEN »	Pour tous les autres versements comme le Service de présentation de factures (SPF).

N103 - N104
Codes inutilisés

PER
Contact pour les communications administratives

Ce code désigne la personne ou le service à contacter pour les questions administratives. Le RG ne tiendra pas compte des données acheminées dans ce segment.

ACT
Désignation du compte

Ce code précise l'information sur le compte.

ACT		ACT01 508 Numéro du compte O AN 10/21		ACT02 93 Nom F AN 1/35		ACT03 66 Qual. du code d'ID C ID 1/2		ACT04 67 Code d'ID C ID 2/17
	*		*		*		*	

*	ACT05 569 Qual. du nº de compte C ID 1/3	*	ACT06 508 Numéro du compte C AN 1/35	*	ACT07 3 Message à struct. non imposée F AN 1/60	N / L

ACT01 - Numéro du compte
Ce numéro désigne l'IF et correspond au numéro de transit et au numéro du compte dans lequel le solde est rapporté.
Ce champ se divise comme suit :

- numéro d'ID ACP de l'IF car. 1 - 4;
- numéro de transit ACP car. 5 - 9;
- numéro du compte car. 10 - 21;

Remarque : le numéro de l'IF, de transit et de compte doit être constitué de zéros et être justifié à droite.

Exemples :
numéro ID ACP de l'IF : 0001
numéro de transit ACP : 9999
numéro du compte du RG : 1234

ACT01 = 000109999000000001234

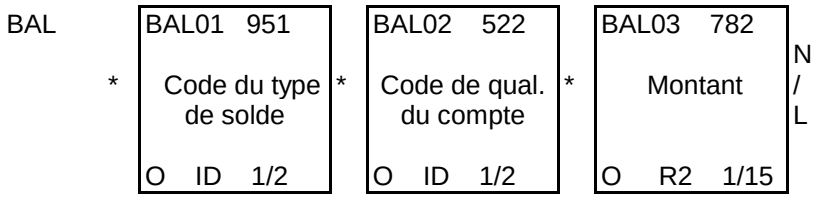
ACT02 - ACT07
Codes inutilisés

CUR
Devise

Ce code désigne la devise employée dans l'opération. Le RG ne tiendra pas compte des données acheminées dans ce segment.

BAL
Détails du solde

Ce code désigne le solde correspondant à un compte en particulier.



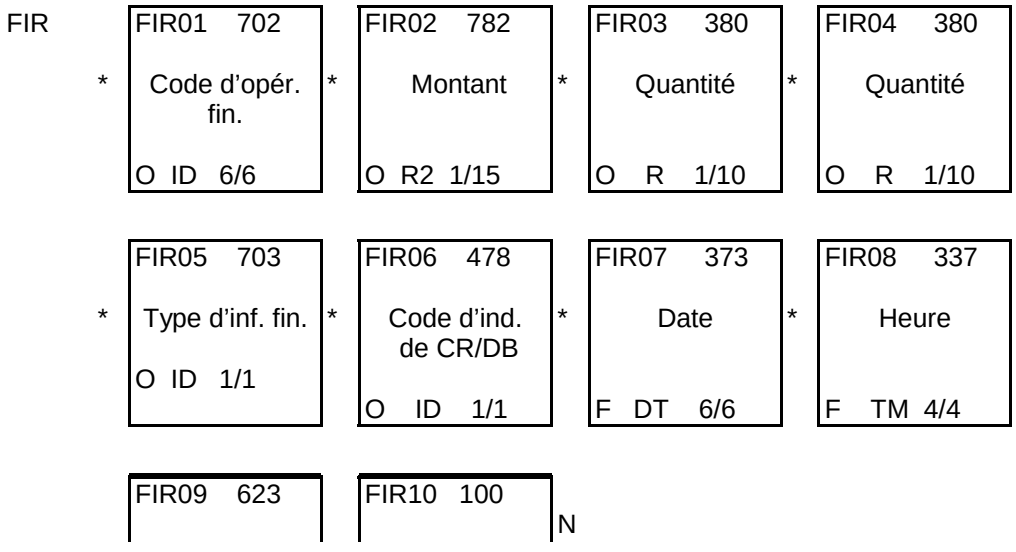
BAL01 Code du type de solde
Le code " Y " (cumul de l'année) indique le solde à jour ou actuel.

BAL02 Ce code qualifie le montant indiqué dans BAL03.
Le code " IB " désigne le " solde à investir " (c'est-à-dire le solde disponible); le code " NL " représente un solde négatif dans le grand livre.

BAL03 Ce code est qualifié par le code dans BAL02.
Il désigne le solde du compte.

FIR
Information financière

Il s'agit du sommaire d'un certain nombre d'opérations de crédit ou de débit d'un compte.



*	Code horaire F ID 2/2	*	Code de devise F ID 3/3	/	L

FIR01 - Ce code désigne le type d'opération. Il faut dresser la liste des codes et des définitions. On doit prévoir des codes distincts pour :

- les opérations relatives à des virements à la Banque du Canada ou entre les sous-comptes et le compte concentrateur;
- les virements télégraphiques;
- les rajustements bancaires relatifs à des virements télégraphiques;
- les dépôts directs;
- les rajustements bancaires relatifs aux dépôts directs.

FIR02 - Montant de l'opération
Ce montant doit toujours être positif; le FIR06 indique s'il s'agit d'un crédit ou d'un débit.

FIR03 - Quantité
Nombre de transactions incluses dans le montant de l'opération posté sous FIR02 (dépôts, etc...)

FIR04 Valeur recommandée : " 1 "

FIR05 - Ce code indique s'il s'agit de renseignements financiers détaillés ou sommaires.
Il doit toujours être égal à " 1 " (" Détails ").

FIR06 - Ce code indique si le FIR02 a porté au compte un crédit ou un débit.
Le code " C " désigne un crédit, et le code " D ", un débit.

FIR07 - Date de valeur de l'opération (AAMMJJ)

FIR08 - FIR09
Codes inutilisés

FIR10 - Code de devise
Code du pays de la devise dans laquelle les frais sont indiqués

REF
Numéros de référence

REF		REF01 128		REF02 127		REF03 352		N
	*	Qual. du num. de référence O ID 2/2	*	Numéro de référence O AN 1/30	*	Description C AN 1/80	/	L

Le RG contrôle la concordance de l'information sur les dépôts, d'après le contenu du segment REF et ce, sous réserve du type de données transmises. Le seul cas dans lequel un segment REF n'est pas nécessaire est celui des virements à la Banque du Canada. Le tableau ci-après fait état des exigences pour chaque type de données.

Type d'état de compte (821)	O Ou F	REF01 (1ère occurrence)	REF02 (1ère occurrence)	O ou F	REF01 (2e occurrence)	REF02 (2e occurrence)
Formulaires 820 ou 823 conformes H6. BGN = 22 (dépôts et rajustements bancaires pour renverser un dépôt)	O	RR ou ZZ	Numéro exclusif de renvoi croisé, qui figure également dans le formulaire 820/823. La longueur de ce numéro peut varier.	O	PQ	Numéro « NIEC » de huit chiffres, attribué par l'ACP
(Effets retournés dans les cas autorisés et rajustements bancaires pour renverser un effet retourné)	F	IX	Numéro exclusif de renvoi croisé dont la longueur peut varier (par exemple, le numéro du client)	O	PQ	Numéro « NIEC » de huit chiffres attribué par l'ACP
Formulaires 820 ou 823 distinct des formulaires ci-dessus et dans lesquels BGN01 = 00/22 (dépôts et rajustements bancaires pour renverser un dépôt)	O	RR ou ZZ	Numéro exclusif de renvoi croisé, qui figure également dans le formulaire 820/823. La longueur de ce numéro peut varier.	O	IT	Numéro d'autorisation du RG de huit chiffres
(Effets retournés dans les cas autorisés et rajustements bancaires pour renverser un effet retourné)	F	IX	Numéro exclusif de renvoi croisé dont la longueur peut varier (par exemple, le numéro du client)	O	IT	Numéro d'autorisation du RG de huit chiffres
Opérations électroniques par carte. BGN01 = 22 (Dépôts et rajustements bancaires pour renverser un dépôt)	O	IX	Numéro de suivi exclusif, dont la longueur peut varier (par exemple, un numéro de fin de lot)	O	VR	Numéro du marchand associé avec le type de carte de la transaction (dont la longueur peut varier)
(Effets retournés dans les cas autorisés et rajustements bancaires pour renverser un effet retourné)	O	IX	Numéro de suivi exclusif, dont la longueur peut varier (par exemple, un numéro de client)	O	VR	Numéro du marchand associé avec le type de carte de la transaction (dont la longueur peut varier)
Comptes de dépôt. BGN01 = 22 (Dépôts et rajustements bancaires pour renverser un dépôt)	O	PB	Numéro de transit de cinq chiffres de la succursale d'origine	O	IT	Numéro d'autorisation du RG de huit chiffres
(Effets retournés dans les cas autorisés et rajustements bancaires pour renverser un effet retourné)	O	PB	Numéro de transit de cinq chiffres de la succursale d'origine	O	IT	Numéro d'autorisation du RG de huit chiffres
Virements à la Banque du Canada	F					
Virements télégraphiques / STPGV	F	IX	Numéro de suivi exclusif, dont la	O	IT	Numéro

(Dépôts et rajustements bancaires)			longueur peut être variable (par exemple, le nº SWIFT)			d'autorisation du RG de huit chiffres
Dépôts directs (Dépôts et rajustements bancaires)	F	IX	Numéro de suivi exclusif, dont la longueur peut varier (par exemple, le nº du fichier des dépôts directs)	O	IT	Numéro d'autorisation du RG de huit chiffres

Numéros d'autorisation, de commerçant, de transit et de créancier ministériel (NIEC)

Les rajustements relatifs aux valeurs des éléments suivants doivent comprendre le numéro de suivi des écritures passées à l'origine pour les dépôts.

IT Ce code constitue, pour le RG, le numéro d'autorisation de huit chiffres désignant le bureau ministériel auquel on doit faire parvenir l'avis d'opération. Ce numéro est fourni à l'IF par l'émetteur de l'opération. REMARQUE : les rajustements et les effets retournés doivent comprendre le numéro d'autorisation du RG de huit chiffres pour les écritures passées à l'origine pour les dépôts.

PB Ce numéro représente, pour le RG, le numéro de transit de la succursale qui a effectué l'opération à l'origine. Ce numéro doit comprendre cinq caractères.

NOTE : REF03 - Description pour les Services d'acceptation des cartes.
Pour la 1ère occurrence: Si REF01 est égal à "IX", REF03 est vide.
Pour la 2e occurrence: Si REF01 est égal à "VR", REF03 doit être le type de carte "VISA", "M/C", "AMEX" ou "DCARD".
Pour les autres services - codes inutilisés.

SE
Segment fin du document informatisé

Ce code désigne la fin du document informatisé.

SE		SE01 96		SE02 329	
	*	Nombre de segments inclus	*	Nº de contrôle du doc. informatisé	N / L
		O NO 1/6		O AN 4/9	

SE01 - Nombre de segments inclus
Cette valeur doit être égale au nombre de segments du document informatisé.

SE02 - Numéro de contrôle du document informatisé
Ce numéro est défini par l'expéditeur; il doit correspondre au numéro de contrôle du document informatisé dans le ST.

ANNEXE A, APPENDICE 5

EXIGENCES DE LA BANQUE DU CANADA EN MATIÈRE DE FORMATAGE EN CE QUI A TRAIT AUX STPGV

Code de la zone SWIFT	Nom de la zone SWIFT	Renseignements exigés par la Banque du Canada
20	Client Reference	Govt EFT
23B	Bank Operation Code	CRED
32A	Value date, Currency, Settlement Amount	
50A	Ordering Customer	BIC of Contractor
57A	Account with Institution	BOC BIC
59	Beneficiary Customer	RG Account No. With BoC Receiver General
72	Bank to Bank Information	/ACC/560: or /BNF/560: or /REC/560:

ANNEXE A, APPENDICE 6

TEF RÉTROSPECTIFS ET PRÉVUS

(Voir le tableur ci-joint)

ANNEXE A, APPENDICE 7

VALEURS ET VOLUMES PRÉVUS DES REMISES POUR 2014 À 2018

(Voir le tableur ci-joint)

ANNEXE A, APPENDICE 7.1

TRANSACTIONS DE PLUS DE 50 M$ PRÉVUES – DÉPÔTS DIRECTS ET VIREMENTS TÉLÉGRAPHIQUES

	Total
Année 1 (2013-2014)	$10,549,423,473
Année 2 (2014-2015)	$11,076,894,647
Année 3 (2015-2016)	$11,630,739,379
Année d'option 1 (2016-2017)	$12,212,276,348
Année d'option 2 (2017-2018)	$12,822,890,165

Veuillez noter que le RG a préparé les prévisions au meilleur de sa connaissance.

ANNEX A, APPENDICE 8

FORMULAIRE DE DEMANDE DE TEF

TYPE DE CONFIGURATION (cocher une case):Nouvelle configuration Modification Fermeture

PARTIE 1 : RENSEIGNEMENTS SUR LE BUREAU MINISTÉRIEL

Nom du ministère :	**Numéro du ministère :**	**Code de région :**
Description du programme :		
Date de mise en œuvre demandée :		

1.1 Renseignements sur l'emplacement du bureau ministériel:

Nom du bureau ministériel (faisant affaire sous le nom de): (bilingue, maximum de 30 caractères, nom de bénéficiaire qui figure sur les instructions de paiement pour les dépôts directs et les virements télégraphiquese entrants)

Adresse:	**Ville et province**	**Code postal:**
Personne-ressource principale		
Nom:	**Numéro de téléphone:**	**Numéro de télécopieur:**
Poste de la personne-ressource:		
Adresse Électronique:		
Autre personne-ressource		
Nom:	**Numéro de Téléphone:**	**Numéro de télécopieur:**
Poste de la personne-ressource:		
Adresse électronique:		

Renseignements sur les transactions:

Nombre de transactions mensuelles prévu:	**Valeur des transactions mensuelles prévue:**

PART 2: RENSIGNEMENTS BANCAIRES

La présente section doit être remplie par le receveur général et l'institution financière dans le cas de NOUVEAUX services, et par le ministère pour effectuer des MODIFICATIONS OU UNE FERMETURE.

Numéro d'autorisation du receveur général:	**Numéro de compte auxiliaire attribué par l'institution financière:**	**Date d'entrée en vigueur:**

Renseignement sur l'institution financière

Fournisseur de services de transfert électronique de fonds actuel:	**Noméro transitaire:**	
Adresse:	**Ville et province:**	**Code postal:**

PART 3: CONFIGURATION DES UTILISATEURS DE L'OUTIL DE RAPPORTS EN LIGNE

Premier utilisateur	
Nom :	**Langue de préférence:** Anglais Français
Numéro de téléphone:	**Numéro de télécopieur:**
Adresse électronique:	
Deuxième utilisateur	
Nom :	**Langue de préférence:** Anglais Français
Numéro de téléphone:	**Numéro de télécopieur:**
Adresse électronique:	

Instructions de configuration des utilisateurs de l'outil de rapports en ligne

[INSÉRER LES DIRECTIVES LORS DE L'ATTRIBUTION DU CONTRAT]

PARTIE 4 : AUTORISATION

REPRÉSENTANT DU RECEVEUR GÉNÉRAL	
Nom:	
Titre:	
Adresse électronique :	
Numéro de téléphone :	**Numéro de télécopieur :**
Signature:	**Date :**
AGENT DE L'INSTITUTION FINANCIÈRE	
Nom:	
Titre:	
Date:	
Signature:	
Date de l'entrée en vigueur :	

Description des zones

Nom de la zone	Explication
Type de configuration	
Type: Nouvelles configuration, modification, fermeture	**Cocher l'option appropriée:** • Nouvelle configuration: Création d'un service de transfert électronique de fonds pour la première fois. • Modification: Modification de la configuration d'un service de transfert électronique de fonds existant. • Fermeture: Fermeture d'un service de transfert électronique de fonds existant.
PART IE 1: RENSEIGNEMENTS SUR LE BUREAU MINISTÉRIEL	
Nom du ministère, numéro du ministère et code de région	Saisir le nom officiel du ministçre, son numéro a trois chiffres et son code de région à trois chiffres, le cas échéant.
Description du programme	Si les services sont utilisés dans le cadre d'un programme précis, décrire ce dernier brièvement. Autrement, ne pas remplir cette zone
Date de mise en oeuvre demandée	Saisir la date de mise en œuvre demandée des services. Il convient de noter que le processus de configuration peut prendre de deux à six semaines. Le ministère doit donc veiller à ce que le formulaire de configuration soit envoyé six semaines avant la date de mise en œuvre demandée. Dans le cas contraire, le receveur général ne pourra pas guarantir le respect de cette date.
Renseignements sur l'emplacement du bureau ministériel	
Nom du bureau ministériel (s/n)	Nom de bénéficiaire qui figure sur les instructions de paiement pour les dépôts directs et les virements télégraphiques entrants. Il devrait être bilingue et être composé d'au plus 30 caractères. Il s'agit en somme du nom sous lequel le bureau fait affaire (s/n).
Adresse et coordonnées des deux personnes-ressources	Adresse et coordonnées des deux personnes-ressources avec lesquelles il faut communiquer pour obtenir du soutien continu.
Renseignements sur les Transactions:	Remplir toutes les zones.
PARTIE 2: RENSEIGNEMENT BANCAIRES	
Numéro d'autorisation du receveur général	En ce qui concerne les nouvelles demandes, le receveur général saisira le numéro d'autorisation. Pour les autres demandes, inscrire le numéro d'autorisation fourni précédemment par le receveur général.
Numéro de compte auxiliaire attribué par l'institution financière	L'institution financière saisira le numéro de compte auxiliaire connexe pour les nouvelles configurations. Le ministère devra renseigner cette zone pour effectuer des modifications ou une fermeture.

Date d’entrée en vigueur	Date à laquelle la demande doit entrer en vigueur. Cette zone doit tre renseignée par le représentant du receveur général.
Financial Institution Information	Inclut le nom et l'adresse de l'institution financière, et le numéro transitaire.
PARTIE 3: CONFIGURATION DES UTILISATEURS DE L’OUTIL DE RAPPORTS EN LIGNE	
Nom, numéro de téléphone, numéro de télécopieur, adresse électronique	Inscrire les coodonnées de l’utilisateur.
Langue de préférence	La solution de rapports en ligne sera affichée dans la langue que l’utilisateur aura choisie.
PARTIE 4: AUTORISATION	
Représentant autorisé par le receveur général	Le représentant autorisé par le receveur général validera l’information.

ANNEXE B

BASE DE PAIEMENT

Période du contrat : La durée du contrat sera de trois ans à compter de la date d'attribution. Pendant la période du contrat, l'entrepreneur sera payé conformément à ce qui est précisé ci-dessous pour tous les travaux réalisés conformément au contrat.

1.0 Frais de transaction

Frais de transaction fermes tout compris par remise de TEF

FRAIS DE TRANSACTION FERMES TOUT COMPRIS APPLICABLES AUX DÉPÔTS DIRECTS ET AUX VIREMENTS TÉLÉGRAPHIQUES					
Catégorie	**Année 1**	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
Dépôt direct					
Frais de transaction fermes tout compris	$	$	$	$	$
Virement télégraphique					
Frais de transaction fermes tout compris	$	$	$	$	$

Si une période de transition est requise, les frais pour cette période seront identiques aux frais en vigueur au moment de l'émission de l'avis de la période de transition.

2.0 Frais uniques pour l'établissement de bureaux ministériels

Il s'agit des frais servant à l'établissement et au maintien de bureaux ministériels ayant la capacité de recevoir des remises de TEF. Ces frais couvrent toutes les activités administratives nécessaires pour que cette capacité soit mise en œuvre.

	Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
Frais uniques fermes tout compris pour l'établissement de bureaux ministériels	**$**	**$**	**$**	**$**	**$**

Si une période de transition est requise, les frais pour cette période seront identiques aux frais en vigueur au moment de l'émission de l'avis de la période de transition.

3.0 Frais mensuels pour l'accès en ligne des utilisateurs ministériels

Il s'agit de frais qui servent à l'établissement et au maintien d'une capacité d'accès en ligne au compte pour chaque employé désigné par les bureaux ministériels. Ces frais couvrent toutes les activités administratives nécessaires pour fournir cette capacité.

	Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
Frais mensuels fermes tout compris pour l'accès en ligne des utilisateurs ministériels (par utilisateur)	**$**	**$**	**$**	**$**	**$**

Si une période de transition est requise, les frais pour cette période seront identiques aux frais en vigueur au moment de l'émission de l'avis de la période de transition.

4.0 Frais accessoires applicables aux transactions d'une valeur égale ou supérieure à 50M$

Un taux ferme fondé sur des points de base sera appliqué à chaque transaction dont la valeur est égale ou supérieure à 50 M$. Puisque l'entrepreneur doit transférer les fonds au compte du RG ouvert à la Banque du Canada le jour de leur réception, s'ils ont été reçus avant 14 h HAE, ou le jour suivant leur réception, s'ils ont été reçus après 14 h HAE, nous sommes conscients que des frais accessoires pourraient devoir être versés lorsque des paiements de grande valeur sont reçus. C'est pourquoi nous avons prévu une méthode par laquelle l'entrepreneur pourra réclamer des frais accessoires relativement à chaque transaction dont la valeur est égale ou supérieure à 50 M$.

	Année 1	**Année 2**	**Année 3**	**Année d'option 1**	**Année d'option 2**
Taux ferme tout compris fondé sur des points de base applicable aux transactions dont la valeur est égale ou supérieure à 50 M$					

Si une période de transition est requise, les frais pour cette période seront identiques aux frais en vigueur au moment de l'émission de l'avis de la période de transition.

5.0 Coût total estimatif - période du contrat : _____$. Les droits de douane sont inclus, et la taxe sur les produits et services (TPS) ou la taxe de vente harmonisée (TVH) est en sus, s'il y a lieu.

6.0 Coût total estimatif - période de prolongation du contrat (de_____ à _____) :
_____ **$.** Les droits de douane sont inclus, et la TPS ou la TVH est en sus, s'il y a lieu.

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
EN89132308
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: Public Works and Government Services Canada	2. Branch or Directorate / Direction générale ou Direction: 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 Electronic Funds Transfer (EFT) services to participating government departments and agencies 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 ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN89132308
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 ☑ / Yes ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — Non ☑ / Oui ☐
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

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

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

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

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

☑ 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 ☑ / Yes ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ☑ / Oui ☐
If Yes, will unscreened personnel be escorted? — No ☑ / Yes ☐
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non ☑ / Oui ☐

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ☐ / Yes ☑
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? — Non ☐ / Oui ☑

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN89132308
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?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, 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).

ANNEXE A, APPENDICE 6.1

VALEURS ET VOLUMES RÉTROSPECTIFS - DÉPÔTS DIRECTS (DD) ET VIREMENTS TÉLÉGRAPHIQUES (VT)

	D'avril 2010 à mars 2011			
	DD		VT	
	Volume	Valeur	Volume	Valeur
0 $ < Valeur < 1 M$	1,822	$60,978,112	3,123	$593,539,481
1 M$ < Valeur < 5 M$	53	$132,651,645	404	$916,045,211
5 M$ < Valeur < 10 M$	12	$82,414,381	75	$529,139,986
10 M$ < Valeur < 50 M$	6	$98,025,661	65	$1,305,877,605
50 M$ et +	2	$130,000,000	36	$5,582,484,864
Total	1,895	$504,069,800	3,703	$8,927,087,147

	D'avril 2011 à mars 2012			
	DD		VT	
	Volume	Valeur	Volume	Valeur
0 $ < Valeur < 1 M$	4,796	$167,618,241	12,931	$987,801,964
1 M$ < Valeur < 5 M$	142	$339,865,441	552	$1,299,412,637
5 M$ < Valeur < 10 M$	24	$164,320,139	113	$819,362,302
10 M$ < Valeur < 50 M$	43	$814,933,779	136	$2,704,142,700
50 M$ et +	11	$962,221,157	51	$8,606,416,913
Total	5,016	$2,448,958,757	13,783	$14,417,136,517

	D'avril 2012 à janvier 2013			
	DD		VT	
	Volume	Valeur	Volume	Valeur
0 $ < Valeur < 1 M$	4,894	$176,120,022	15,399	$907,186,083
1 M$ < Valeur < 5 M$	138	$359,057,816	507	$1,109,554,327
5 M$ < Valeur < 10 M$	40	$285,643,762	92	$640,946,643
10 M$ < Valeur < 50 M$	40	$863,801,493	118	$2,319,059,229
50 M$ et +	4	$308,822,761	45	$6,819,727,280
Total	5,116	$1,993,445,854	16,161	$11,796,473,563

Détails des transactions de plus de 50 M$		
Date (JJ/MM/AAAA)	Type de transaction	Montant
01/12/2010	VT	$ 50,138,914.94
31/03/2011	VT	$ 50,683,262.00
12/08/2010	VT	$ 51,021,250.00
12/08/2010	VT	$ 51,058,000.00
12/08/2010	VT	$ 51,060,000.00
01/10/2010	VT	$ 53,904,980.58
23/09/2010	VT	$ 62,771,212.64
11/03/2011	DD	$ 65,000,000.00
11/03/2011	DD	$ 65,000,000.00
13/04/2010	VT	$ 75,000,000.00
23/06/2010	VT	$ 76,539,000.00
26/01/2011	VT	$ 77,849,732.92
01/03/2011	VT	$ 80,480,142.82
01/10/2010	VT	$ 81,015,572.86
01/03/2011	VT	$ 82,718,712.79
21/03/2011	VT	$ 96,236,659.27
01/10/2010	VT	$ 98,520,000.00
03/08/2010	VT	$ 100,000,000.00
21/03/2011	VT	$ 102,044,500.00
21/03/2011	VT	$ 102,147,000.00
01/10/2010	VT	$ 106,618,520.44
01/10/2010	VT	$ 107,669,271.58
01/03/2011	VT	$ 117,839,855.96
01/03/2011	VT	$ 118,153,920.86
01/03/2011	VT	$ 122,159,993.21
31/03/2011	VT	$ 124,214,142.27
30/09/2010	VT	$ 125,235,036.35
01/10/2010	VT	$ 145,717,080.20
13/04/2010	VT	$ 150,000,000.00
31/12/2010	VT	$ 154,765,755.42
30/06/2010	VT	$ 156,892,200.21
01/10/2010	VT	$ 248,909,159.38
01/06/2010	VT	$ 303,414,799.82
13/04/2010	VT	$ 325,000,000.00
17/03/2011	VT	$ 350,000,000.00
31/03/2011	VT	$ 353,300,296.00
31/03/2011	VT	$ 496,000,000.00
20/04/2010	VT	$ 733,405,891.07

Détails des transactions de plus de 50 M$		
Date (JJ/MM/AAAA)	Type de transaction	Montant
27/10/2011	VT	$ 50,000,000.00
27/10/2011	VT	$ 50,000,000.00
30/06/2011	VT	$ 50,082,778.00
30/03/2012	VT	$ 50,295,241.42
22/11/2011	VT	$ 50,464,348.00
30/03/2012	DD	$ 51,165,618.88
18/11/2011	DD	$ 51,620,713.01
01/12/2011	VT	$ 55,104,292.50
30/06/2011	VT	$ 55,487,429.32
29/06/2011	VT	$ 57,000,000.00
30/03/2012	VT	$ 58,821,932.61
21/03/2012	VT	$ 63,508,341.17
19/07/2011	VT	$ 65,427,973.00
14/02/2012	VT	$ 68,961,892.90
01/06/2011	VT	$ 70,496,491.06
01/06/2011	VT	$ 79,794,407.53
01/09/2011	VT	$ 79,952,143.78
01/09/2011	DD	$ 79,952,143.78
31/08/2011	VT	$ 80,000,000.00
02/12/2011	DD	$ 80,100,000.00
20/09/2011	DD	$ 80,211,144.00
17/06/2011	DD	$ 80,275,000.00
16/03/2012	VT	$ 82,978,510.89
04/11/2011	VT	$ 83,000,000.00
28/02/2012	DD	$ 84,100,000.00
15/03/2012	VT	$ 85,180,677.00
19/03/2012	VT	$ 87,166,148.92
30/03/2012	VT	$ 91,159,217.77
30/03/2012	DD	$ 93,418,277.10
01/06/2011	VT	$ 93,888,718.45
11/04/2011	VT	$ 99,477,500.00
01/06/2011	VT	$ 106,441,246.15
11/04/2011	VT	$ 109,855,608.22
01/09/2011	VT	$ 116,094,789.05
01/09/2011	DD	$ 116,094,789.05
01/09/2011	VT	$ 116,287,059.45
01/06/2011	VT	$ 118,086,223.89
18/04/2011	VT	$ 122,057,718.29
01/09/2011	VT	$ 122,252,672.72
01/09/2011	DD	$ 122,252,672.72

Détails des transactions de plus de 50 M$		
Date (JJ/MM/AAAA)	Type de transaction	Montant
29/11/2012	DD	$ 51,353,032.07
24/05/2012	VT	$ 52,842,600.00
20/06/2012	VT	$ 52,925,000.00
12/10/2012	VT	$ 54,906,597.00
11/12/2012	VT	$ 55,000,000.00
01/06/2012	VT	$ 60,087,162.86
12/07/2012	VT	$ 60,352,717.02
01/06/2012	VT	$ 61,133,515.16
01/06/2012	VT	$ 62,414,819.08
20/11/2012	VT	$ 64,233,841.52
27/12/2012	VT	$ 64,242,432.09
29/06/2012	VT	$ 68,623,566.00
31/05/2012	VT	$ 70,344,393.70
01/06/2012	VT	$ 72,096,108.79
20/04/2012	VT	$ 80,251,247.95
06/12/2012	DD	$ 84,175,000.00
15/10/2012	DD	$ 85,919,729.00
18/06/2012	DD	$ 87,375,000.00
20/04/2012	VT	$ 89,833,379.38
01/06/2012	VT	$ 95,216,451.42
01/06/2012	VT	$ 96,256,650.66
01/06/2012	VT	$ 96,462,352.99
31/05/2012	VT	$ 97,220,970.80
01/06/2012	VT	$ 101,893,855.26
01/10/2012	VT	$ 115,662,102.55
02/04/2012	VT	$ 119,430,202.84
01/06/2012	VT	$ 122,032,155.92
01/06/2012	VT	$ 122,276,062.44
01/06/2012	VT	$ 123,256,983.14
31/12/2012	VT	$ 141,824,423.21
03/07/2012	VT	$ 143,033,276.31
18/06/2012	VT	$ 210,343,327.93
01/06/2012	VT	$ 213,459,306.83
15/06/2012	VT	$ 226,357,165.38
01/06/2012	VT	$ 232,344,615.29
01/06/2012	VT	$ 239,854,399.85
01/06/2012	VT	$ 240,789,043.37
13/04/2012	VT	$ 248,237,091.39
09/04/2012	VT	$ 249,156,669.20
09/04/2012	VT	$ 250,872,931.64

30/09/2011	VT	$ 122,574,369.48
01/09/2011	VT	$ 123,030,798.92
01/09/2011	DD	$ 123,030,798.92
01/06/2011	VT	$ 124,777,442.89
01/06/2011	VT	$ 135,251,130.57
16/06/2011	VT	$ 135,268,968.98
01/06/2011	VT	$ 147,180,702.01
30/06/2011	VT	$ 149,388,324.02
21/11/2011	VT	$ 160,402,213.46
01/06/2011	VT	$ 179,079,575.96
01/06/2011	VT	$ 211,311,537.92
03/01/2012	VT	$ 212,684,770.44
30/03/2012	VT	$ 319,800,000.00
01/06/2011	VT	$ 328,123,931.76
21/12/2011	VT	$ 340,100,000.00
01/04/2011	VT	$ 346,799,000.00
30/03/2012	VT	$ 362,792,452.00
01/06/2011	VT	$ 493,981,043.77
15/03/2012	VT	$ 500,000,000.00
24/05/2011	VT	$ 500,000,000.00
24/05/2011	VT	$ 634,018,507.58
30/03/2012	VT	$ 660,528,781.41

01/06/2012	VT	$ 281,910,909.22
07/05/2012	VT	$ 300,947,533.86
01/06/2012	VT	$ 324,785,990.63
02/04/2012	VT	$ 371,616,000.00
01/06/2012	VT	$ 397,600,292.50
01/06/2012	VT	$ 438,273,453.86
09/01/2013	VT	54,560,000
10/01/2013	VT	74,356,667.63
21/01/2013	VT	120,409,013.18

ANNEXE A, APPENDICE 6.2

VOLUMES HEBDOMADAIRES DES VIREMENTS TÉLÉGRAPHIQUES ENTRANTS

Légende :

	Semaine chevauchant deux mois								
Période	D'avril 2010 à mars 2011			D'avril 2011 à mars 2012			D'avril 2012 à mars 2013		
Mois	Sem.	Nbre de VT	Montant total	Sem.	Nbre de VT	Montant total	Sem.	Nbre de VT	Montant total
Avril	5 AV	5	$ 1,206,391	1	124	$ 50,415,652	1	311	$ 538,559,835
	1	28	$ 10,230,205	2	130	$ 226,473,862	2	286	$ 790,462,987
	2	34	$ 562,410,143	3	181	$ 205,171,569	3	366	$ 311,416,478
	3	32	$ 743,692,461	4	326	$ 278,196,270	4	584	$ 71,822,889
	4	26	$ 84,873,815				5 AV	208	$ 171,614,913
							5 M	280	$ 39,392,559
	Total	125	$ 1,402,413,015	Total	761	$ 760,257,353	Total	2,035	$ 1,923,269,661
Mai	1	41	$ 12,489,537	1	244	$ 56,803,415	1	222	$ 370,506,022
	2	49	$ 22,466,760	2	163	$ 15,278,881	2	297	$ 77,758,742
	3	26	$ 9,616,207	3	187	$ 113,912,756	3	311	$ 176,491,425
	4	49	$ 20,477,803	4	190	$ 1,183,071,749	4 M	290	$ 403,609,012
	5 M	34	$ 41,050,947	5 M	93	$ 143,940,495	4 JN	106	$ 3,461,715,714
	5 JN	43	$ 324,275,856	5 JN	148	$ 2,229,906,314			
	Total	242	$ 430,377,110	Total	1,025	$ 3,742,913,611	Total	1,226	$ 4,490,080,915
Juin	1	61	$ 12,789,108	1	166	$ 11,748,312	1	204	$ 11,855,703
	2	50	$ 25,942,695	2	202	$ 230,159,685	2	265	$ 255,628,017
	3	77	$ 102,440,584	3	202	$ 47,439,247	3	299	$ 376,411,879
	4 JN	52	$ 230,114,336	4	252	$ 489,346,507	4	474	$ 319,684,162
	4 JL	20	$ 9,526,142						
	Total	260	$ 380,812,866	Total	822	$ 778,693,751	Total	1,242	$ 963,579,761
Juillet	1	48	$ 59,971,997	1	208	$ 77,342,426	1	284	$ 265,420,357
	2	63	$ 30,087,275	2	218	$ 27,603,067	2	295	$ 215,790,772
	3	85	$ 93,914,977	3	244	$ 234,206,795	3	392	$ 188,346,950
	4	49	$ 53,254,393	4	383	$ 138,697,708	4	515	$ 74,200,589
							5 JL	330	$ 144,131,787
							5 AO	233	$ 46,162,175
	Total	245	$ 237,228,642	Total	1,053	$ 477,849,995	Total	2,049	$ 934,052,630
Août	1	45	$ 121,311,557	1	224	$ 50,210,282	1	228	$ 17,805,576
	2	48	$ 214,345,522	2	143	$ 49,269,955	2	284	$ 78,871,226
	3	77	$ 72,749,659	3	213	$ 19,204,563	3	287	$ 100,285,459
	4	28	$ 10,102,830	4	212	$ 99,783,480	4	392	$ 181,980,295
	5 AO	21	$ 36,113,198	5 AO	197	$ 268,259,631			
	5 S	45	$ 36,920,976	5 S	96	$ 587,324,922			
	Total	264	$ 491,543,742	Total	1,085	$ 1,074,052,834	Total	1,191	$ 378,942,555
Septembre	1	27	$ 24,665,685	1	144	$ 10,793,932	1	207	$ 27,033,414
	2	58	$ 51,555,230	2	211	$ 67,675,218	2	206	$ 14,101,759
	3	65	$ 127,870,265	3	230	$ 91,710,588	3	352	$ 116,525,348
	4 S	31	$ 192,518,049	4	313	$ 322,091,374	4	464	$ 130,155,784
	4 O	21	$ 855,161,365						
	Total	202	$ 1,251,770,594	Total	898	$ 492,271,113	Total	1,229	$ 287,816,305
Octobre	1	48	$ 17,879,683	1	202	$ 57,911,573	1	259	$ 196,125,254
	2	39	$ 14,888,635	2	197	$ 42,401,775	2	280	$ 80,352,152
	3	73	$ 58,196,936	3	266	$ 87,420,678	3	387	$ 48,013,365

VOLUMES MENSUELS DES VIREMENTS TÉLÉGRAPHIQUES ENTRANTS

Période	2010-2011		2011-2012		2012-2013	
Mois	Nbre de VT	Montant total	Nbre de VT	Montant total	Nbre de VT	Montant total
Avril	125	$ 1,402,413,015	808	$ 1,124,424,514	1,755	$ 1,883,877,102
Mai	199	$ 106,101,254	877	$ 1,513,007,297	1,400	$ 1,067,757,760
Juin	283	$ 695,562,580	970	$ 3,008,600,065	1,348	$ 4,425,295,475
Juillet	265	$ 246,754,784	1,053	$ 477,849,995	1,816	$ 887,890,455
Août	219	$ 454,622,766	989	$ 486,727,912	1,424	$ 425,104,730
Septembre	226	$ 433,530,205	994	$ 1,079,596,034	1,229	$ 287,816,305
Octobre	250	$ 1,134,098,784	1,147	$ 439,764,091	1,865	$ 628,039,259
Novembre	230	$ 263,002,072	1,122	$ 742,227,953	1,513	$ 476,255,896
Décembre	324	$ 775,539,164	1,155	$ 1,104,659,662	1,504	$ 932,317,659
Janvier	313	$ 374,200,449	1,357	$ 679,593,455	2,307	$ 782,118,921
Février	558	$ 324,490,969	1,662	$ 637,424,925		
Mars	711	$ 2,716,771,106	1,649	$ 3,123,260,613		
TOTAL	3,703	$ 8,927,087,147	13,783	$ 14,417,136,518	16,161	$ 11,796,473,563

	4	69	$ 187,972,165	4	366	$ 150,285,251	4	468	$	176,322,828
				5 O	116	$ 101,744,814	5 O	471	$	127,225,660
				5 N	217	$ 180,456,395	5 N	185	$	24,485,118
	Total	229	$ 278,937,419	Total	1,364	$ 620,220,486	Total	2,050	$	652,524,377
Novembre	1	47	$ 14,765,204	1	152	$ 30,408,386	1	261	$	21,639,170
	2	31	$ 5,576,444	2	269	$ 24,667,231	2	332	$	66,837,676
	3	42	$ 11,644,184	3	237	$ 329,762,328	3	274	$	187,059,524
	4	65	$ 75,585,171	4 N	247	$ 176,933,613	4	461	$	176,234,408
	5 N	45	$ 155,431,070	4 D	149	$ 383,149,860				
	5 D	115	$ 393,613,586							
	Total	345	$ 656,615,658	Total	1,054	$ 944,921,418	Total	1,328	$	451,770,778
Décembre	1	39	$ 5,581,937	1	208	$ 11,494,243	1	335	$	327,060,743
	2	59	$ 18,635,859	2	259	$ 58,487,033	2	345	$	137,365,614
	3	62	$ 66,509,177	3	313	$ 517,414,390	3	454	$	140,954,554
	4	49	$ 291,198,605	4	226	$ 134,114,137	4	276	$	118,029,718
							5D	94	$	208,907,031
	Total	209	$ 381,925,578	Total	1,006	$ 721,509,802	Total	1,504	$	932,317,659
Janvier	1	49	$ 24,921,543	1	143	$ 250,519,902	1	217	$	59,260,418
	2	60	$ 25,803,001	2	246	$ 96,513,389	2	484	$	208,767,476
	3	105	$ 106,006,606	3	315	$ 152,375,280	3	512	$	238,626,910
	4	70	$ 96,823,033	4	376	$ 40,146,474	4	544	$	109,013,529
	5 J	29	$ 120,646,265	5 J	277	$ 140,038,411	5 J	550	$	166,450,588
	5 F	84	$ 20,478,536	5 F	260	$ 59,541,636	5 F			
	Total	397	$ 394,678,985	Total	1,617	$ 739,135,091	Total	2,307	$	782,118,921
Février	1	123	$ 11,818,349	1	334	$ 29,390,729	1			
	2	124	$ 17,458,587	2	374	$ 135,458,015	2			
	3	119	$ 74,610,277	3	374	$ 176,730,382	3			
	4 F	108	$ 200,125,220	4 F	320	$ 236,304,163	4 F			
	4 M	105	$ 559,629,119	4 M	170	$ 47,498,906	4 M			
	Total	579	$ 863,641,551	Total	1,572	$ 625,382,195	Total			
Mars	1	107	$ 15,403,089	1	292	$ 11,349,069	1			
	2	161	$ 466,002,526	2	328	$ 807,440,858	2			
	3	163	$ 368,701,404	3	322	$ 272,505,569	3			
	4 M	175	$ 1,307,034,968	4 M	537	$ 1,984,466,211	4 M			
	4 AV	47	$ 364,167,161				4 AV			
	Total	653	$ 2,521,309,148	Total	1,479	$ 3,075,761,707	Total			
GRAND TOTAL	10/11	3,750	$ 9,291,254,308	11/12	13,736	$ 14,052,969,357	12/13	16,161	$	11,796,473,563
GRAND TOTAL RAJUSTÉ*	10/11	3,703	$ 8,927,087,147	11/12	13,783	$ 14,417,136,518	12/13			

* Le rajustement des transactions de l'exercice suivant est compris dans les données de l'exercice courant.

ANNEXE A, APPENDICE 6.3

VOLUMES DES DÉPÔTS DIRECTS ENTRANTS

Légende :

	Semaine comprenant les premiers jours du mois suivant

Période	D'avril 2010 à mars 2011			D'avril 2011 à mars 2012			D'avril 2012 à mars 2013		
Mois	Sem.	Nbre de DD	Montant total	Sem.	Nbre de DD	Montant total	Sem.	Nbre de DD	Montant total
Avril	5 AV	1	$ 806	1	70	$ 10,020,983	1	113	$ 26,596,979
	1	11	$ 351,365	2	68	$ 1,857,945	2	90	$ 6,743,482
	2	13	$ 197,946	3	58	$ 1,681,291	3	86	$ 2,729,008
	3	12	$ 133,125	4	115	$ 19,274,609	4	122	$ 68,498,299
	4	14	$ 1,492,596				5 AV	60	$ 30,192,855
							5 M	101	$ 10,304,606
	Total	51	$ 2,175,836	Total	311	$ 32,834,828	Total	572	$ 145,065,230
Mai	1	34	$ 4,627,781	1	109	$ 29,580,364	1	88	$ 6,900,466
	2	4	$ 4,604	2	66	$ 2,129,730	2	106	$ 15,522,895
	3	18	$ 2,849,083	3	82	$ 27,147,660	3	98	$ 39,472,521
	4	8	$ 72,332	4	59	$ 18,551,875	4 M	112	$ 22,116,474
	5 M	1	$ 2,504,060	5 M	58	$ 31,652,663	4 JN	38	$ 26,497,041
	5 JN	12	$ 634,587	5 JN	53	$ 10,072,499			
	Total	77	$ 10,692,446	Total	427	$ 119,134,791	Total	442	$ 110,509,398
Juin	1	10	$ 289,782	1	79	$ 3,067,861	1	108	$ 13,104,386
	2	25	$ 519,744	2	106	$ 130,048,544	2	107	$ 30,123,239
	3	16	$ 1,448,876	3	77	$ 4,288,303	3	128	$ 201,172,630
	4 JN	20	$ 7,952,475	4	115	$ 32,079,987	4	139	$ 73,805,087
	4 JL	8	$ 3,775,312						
	Total	79	$ 13,986,189	Total	377	$ 169,484,696	Total	482	$ 318,205,343
Juillet	1	14	$ 830,507	1	119	$ 55,928,865	1	116	$ 53,538,503
	2	23	$ 727,955	2	86	$ 1,311,138	2	86	$ 17,613,169
	3	18	$ 616,862	3	118	$ 23,711,612	3	103	$ 29,184,260
	4	27	$ 7,481,891	4	153	$ 18,771,195	4	103	$ 47,498,882
							5 JL	58	$ 15,254,885
							5 AO	75	$ 13,320,516
	Total	82	$ 9,657,215	Total	476	$ 99,722,809	Total	541	$ 176,410,213
Août	1	16	$ 13,615,817	1	131	$ 11,331,908	1	98	$ 14,627,377
	2	22	$ 880,240	2	105	$ 2,022,091	2	91	$ 6,010,690
	3	41	$ 1,108,814	3	115	$ 16,890,460	3	101	$ 47,892,389
	4	25	$ 977,545	4	113	$ 45,890,706	4	136	$ 56,254,235
	5AO	35	$ 8,874,345	5AO	64	$ 15,802,216			
	5S	13	$ 3,866,625	5S	54	$ 452,390,641			
	Total	152	$ 29,323,386	Total	582	$ 544,328,021	Total	426	$ 124,784,691
Septembre	1	19	$ 998,442	1	69	$ 52,259,350	1	84	$ 8,263,693
	2	33	$ 973,780	2	51	$ 1,501,194	2	79	$ 16,275,461
	3	36	$ 2,668,927	3	78	$ 99,155,231	3	132	$ 23,985,002
	4 S	42	$ 1,087,429	4	97	$ 66,770,273	4	141	$ 72,338,884
	4 O	15	$ 7,093,958						
	Total	145	$ 12,822,537	Total	295	$ 219,686,048	Total	436	$ 120,863,040
Octobre	1	31	$ 4,389,760	1	96	$ 15,838,004	1	121	$ 21,404,635
	2	34	$ 296,311	2	64	$ 6,359,282	2	113	$ 7,138,108

Période	2010-2011		2011-2012		2012-2013	
Mois	Nbre de DD	Montant total	Nbre de DD	Montant total	Nbre de DD	Montant total
Avril	51	$ 2,175,836	342	$ 48,191,134	471	$ 134,760,624
Mai	65	$ 10,057,859	374	$ 109,062,293	505	$ 94,316,963
Juin	83	$ 10,845,464	430	$ 179,557,195	520	$ 344,702,384
Juillet	90	$ 13,432,527	476	$ 99,722,809	466	$ 163,089,697
Août	139	$ 25,456,761	528	$ 91,937,380	501	$ 138,105,208
Septembre	143	$ 9,595,203	349	$ 672,076,689	436	$ 120,863,040
Octobre	172	$ 25,622,539	367	$ 113,781,723	587	$ 305,528,092
Novembre	179	$ 39,881,784	429	$ 157,452,115	583	$ 280,541,728
Décembre	180	$ 37,392,423	390	$ 263,124,295	451	$ 301,563,882
Janvier	210	$ 21,549,702	431	$ 167,257,204	596	$ 109,974,236.12
Février	257	$ 97,973,031	422	$ 213,878,396		
Mars	326	$ 210,086,671	478	$ 332,917,528		
TOTAL	1,895	$ 504,069,800	5,016	$ 2,448,958,759	5,116	$ 1,993,445,854

	3	27	$ 1,111,822	3	96	$ 20,640,530	3	119	$ 175,118,324
	4	65	$ 12,730,688	4	87	$ 27,547,743	4	145	$ 56,523,243
				5 O	24	$ 43,396,165	5 O	89	$ 45,343,783
				5 N	74	$ 17,291,192	5 N	77	$ 76,235,746
	Total	157	$ 18,528,581	Total	441	$ 131,072,915	Total	664	$ 381,763,839
Novembre	1	30	$ 8,125,611	1	66	$ 8,090,994	1	110	$ 13,368,147
	2	26	$ 12,775,597	2	109	$ 76,563,062	2	107	$ 43,262,839
	3	44	$ 922,510	3	98	$ 8,304,117	3	126	$ 10,087,771
	4	33	$ 272,477	4 N	82	$ 47,202,749	4	163	$ 137,587,224
	5 N	46	$ 17,785,589	4 D	46	$ 107,486,156			
	5 D	30	$ 14,532,775						
	Total	209	$ 54,414,559	Total	401	$ 247,647,079	Total	506	$ 204,305,982
Décembre	1	27	$ 410,551	1	86	$ 34,723,806	1	141	$ 165,594,710
	2	44	$ 4,879,389	2	94	$ 12,630,904	2	103	$ 74,639,577
	3	44	$ 7,112,770	3	82	$ 82,949,493	3	123	$ 17,275,032
	4	35	$ 10,456,939	4	82	$ 25,333,935	4	57	$ 20,189,911
							5D	27	$ 23,864,652
	Total	150	$ 22,859,648	Total	344	$ 155,638,139	Total	451	$ 301,563,882
Janvier	1	34	$ 4,028,046	1	77	$ 24,977,207	1	81	$ 10,981,102
	2	34	$ 1,808,945	2	89	$ 17,055,323	2	120	$ 9,175,213
	3	46	$ 2,262,219	3	89	$ 17,604,194	3	140	$ 21,584,971
	4	55	$ 6,404,756	4	96	$ 83,704,767	4	129	$ 41,041,383
	5 J	41	$ 7,045,736	5 J	80	$ 23,915,713	5 J	126	$ 27,191,567
	5 F	46	$ 11,824,967	5 F	60	$ 8,855,025			
	Total	256	$ 33,374,669	Total	491	$ 176,112,229	Total	596	$ 109,974,236
Février	1	62	$ 16,615,404	1	83	$ 28,226,445	1		
	2	65	$ 21,031,607	2	104	$ 1,918,312	2		
	3	48	$ 2,796,162	3	81	$ 27,308,500	3		
	4 F	36	$ 45,704,890	4 F	94	$ 147,570,114	4 F		
	4 M	57	$ 7,409,934	4 M	53	$ 48,563,191	4 M		
	Total	268	$ 93,557,998	Total	415	$ 253,586,562	Total		
Mars	1	58	$ 131,064,996	1	100	$ 25,789,199	1		
	2	57	$ 17,835,691	2	93	$ 17,598,368	2		
	3	60	$ 12,521,052	3	96	$ 3,442,661	3		
	4 M	94	$ 41,254,998	4	136	$ 237,524,109	4		
	4 AV	31	$ 15,356,305						
	Total	300	$ 218,033,042	Total	425	$ 284,354,337	Total		
GRAND TOTAL	10/11	1,926	$ 519,426,105	11/12	4,985	$ 2,433,602,454	12/13	5,116	$ 1,993,445,854
GRAND TOTAL RAJUSTÉ*	10/11	1,895	$ 504,069,800	11/12	5,016	$ 2,448,958,759	12/13		

* Le rajustement des transactions de l'exercice suivant est compris dans les données de l'exercice courant.

ANNEXE A, APPENDICE 7

VALEURS ET VOLUMES PRÉVUS - DÉPÔTS DIRECTS ET VIREMENTS TÉLÉGRAPHIQUES

	Exercice 2013-2014				Exercice 2014-2015				Exercice 2015-2016				Exercice 2016-2017				Exercice 2017-2018			
	Nbre de DD	Valeur des DD	Nbre de VT	Valeur des VT	Nbre de DD	Valeur des DD	Nbre de VT	Valeur des VT	Nbre de DD	Valeur des DD	Nbre de VT	Valeur des VT	Nbre de DD	Valeur des DD	Nbre de VT	Valeur des VT	Nbre de DD	Valeur des DD	Nbre de VT	Valeur des VT
Avril	495	$141,498,655	1,843	$1,978,070,957	519	$148,578,588	1,935	$2,076,974,505	545	$156,002,267	2,032	$2,180,823,230	573	$163,802,381	2,133	$2,289,864,392	601	$171,992,500	2,240	$2,404,357,611
Mai	530	$99,032,811	1,470	$1,121,145,648	557	$103,984,452	1,544	$1,177,202,930	585	$109,183,674	1,621	$1,236,063,077	614	$114,642,858	1,702	$1,297,866,231	645	$120,375,001	1,787	$1,362,759,542
Juin	546	$361,937,503	1,415	$4,646,560,249	573	$380,034,378	1,486	$4,878,888,261	602	$399,036,097	1,560	$5,122,832,675	632	$418,987,902	1,639	$5,378,974,308	664	$439,937,297	1,720	$5,647,923,024
Juillet	489	$171,244,182	1,907	$932,284,977	514	$179,806,391	2,002	$978,899,226	539	$188,796,711	2,102	$1,027,844,188	566	$198,236,546	2,207	$1,079,236,397	595	$208,148,374	2,318	$1,133,198,217
Août	526	$145,010,468	1,495	$446,359,967	552	$152,260,991	1,570	$468,677,965	580	$159,874,041	1,648	$492,111,863	609	$167,867,743	1,731	$516,717,456	639	$176,261,130	1,817	$542,553,329
Septembre	458	$126,906,192	1,290	$302,207,121	481	$133,251,501	1,355	$317,317,477	505	$139,914,077	1,423	$333,183,350	530	$146,909,780	1,494	$349,842,518	556	$154,255,269	1,569	$367,334,644
Octobre	616	$320,804,497	1,958	$659,441,222	647	$336,844,722	2,056	$692,413,283	680	$353,686,958	2,159	$727,033,947	714	$371,371,306	2,267	$763,385,645	749	$389,939,871	2,380	$801,554,927
Novembre	612	$294,568,815	1,589	$500,068,691	643	$309,297,255	1,668	$525,072,126	675	$324,762,118	1,751	$551,325,732	709	$341,000,224	1,839	$578,892,019	744	$358,050,235	1,931	$607,836,620
Décembre	474	$316,642,076	1,579	$978,933,542	497	$332,474,180	1,658	$1,027,880,219	522	$349,097,889	1,741	$1,079,274,230	548	$366,552,784	1,828	$1,133,237,942	576	$384,880,423	1,920	$1,189,899,839
Janvier	626	$115,472,948	2,422	$821,224,867	657	$121,246,595	2,543	$862,286,110	690	$127,308,925	2,671	$905,400,416	724	$133,674,371	2,804	$950,670,437	761	$140,358,090	2,944	$998,203,959
Février	465	$235,800,932	1,832	$702,760,980	489	$247,590,978	1,924	$737,899,029	513	$259,970,527	2,020	$774,793,981	539	$272,969,053	2,121	$813,533,680	566	$286,617,506	2,227	$854,210,364
Mars	527	$367,041,574	1,909	$3,443,394,826	553	$385,393,653	2,004	$3,615,564,567	581	$404,663,336	2,105	$3,796,342,796	610	$424,896,503	2,210	$3,986,159,936	641	$446,141,328	2,320	$4,185,467,932
	6,364	2,695,960,653	20,710	16,532,453,048	6,682	2,830,758,686	21,746	17,359,075,700	7,016	2,972,296,620	22,833	18,227,029,485	7,367	3,120,911,451	23,975	19,138,380,959	7,736	3,276,957,024	25,174	20,095,300,007

Veuillez noter que le RG a préparé les prévisions au meilleur de sa connaissance.

Selon les données de 2011-2012 (5 % pour 2012-2013 et 2013-2014)
Selon les données de 2012-2013 (5 % pour 2013-2014)

Attachement 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 transfert électronique de fonds est conforme aux présentes exigences de référence en matière de sécurité de la TI. Dans la mesure où cela s'applique aux solutions de transfert électronique de fonds 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 transfert électronique de fonds proposée.

La démonstration du respect de la base de référence et des exigences supplémentaires applicables précisées ci-dessous, devra être faite à la demande du Canada, après l'attribution du contrat.

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 transfert électronique de fonds, 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;	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
		○ système et acquisition de services; ○ 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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 : o établit un processus d'autorisation du personnel de maintenance et conserve une liste à jour du personnel et des organismes de maintenance autorisés; o 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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 : ○ a recours à des contrôles de sécurité techniques, opérationnels et administratifs pour le système d'information aux lieux de travail secondaires; ○ évalue l'efficacité des contrôles de sécurité dans les lieux de travail secondaires; ○ 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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 : ○ 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 transfert électronique de fonds.

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.	✓	
SC-12-01	CRÉATION ET GESTION	• Le fournisseur de services tient les renseignements à		✓

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	D'UNE CLÉ CRYPTOGRAPHIQUE	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 LE SERVICE DE	Les systèmes d'information qui fournissent collectivement un service de résolution du nom et de l'adresse pour une organisation sont insensibles aux défaillances et appliquent	✓	

Point n°	Titre de l'exigence	Description	Référence	Supplémentaire
	RÉSOLUTION DU NOM ET DE L'ADRESSE	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 transfert électronique de fonds.

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 transfert électronique de fonds.

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 transfert électronique de fonds.

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.	✓	