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

This document contains a Security Requirement

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

Title - Sujet EFT REMITTANCE SERVICE	
Solicitation No. - N° de l'invitation EN891-132308/A	**Date** 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 410zg.EN891-132308	**CCC No./N° CCC - FMS No./N° VME**
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: Gagnon, Jocelyne C.	**Buyer Id - Id de l'acheteur** 410zg
Telephone No. - N° de téléphone (819) 956-0575 ( )	**FAX No. - N° de FAX** (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 See Herein	**Delivery Offered - Livraison proposée**
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**	

Canada

TABLE OF CONTENTS

PART 7 - RESULTING CONTRACT CLAUSES

1. Statement of Work
2. Standard Clauses and Conditions
3. Security Requirement
4. Term of Contract
5. Authorities
6. Payment
7. Invoicing Instructions
8. Certifications
9. Applicable Laws
10. Priority of Documents
11. Foreign Nationals (Canadian Contractor) and/or Foreign Nationals (Foreign Contractor)
12. Insurance

List of Annexes:

Annex A Statement of Work
Annex B Basis of Payment
Annex C Security Requirements Check List
- Attachment 1 to Annex “C”, Information Technology Security Requirements (ITSR) Technical Document

PART 1 - GENERAL INFORMATION

1. Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation ;

Part 3 Bid Preparation Instructions: provides bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications: includes the certifications to be provided;

Part 6 Security and Financial Requirements: includes specific requirements that must be addressed by bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Attachments include Pricing Schedule, Technical Criteria and Certifications Precedent to Contract Award.

The Annexes include the Statement of Work, Basis of Payment and Security Requirements Check List.

2. Summary

2.1 The Department of Public Works and Government Services Canada (PWGSC) on behalf of the Receiver General for Canada requires a formal arrangement with a single service provider for incoming Electronic Fund Transfer Service (EFT). This service is to cover payments made to the government by direct deposit and wire transfer that are denominated in Canadian dollars.

Currently, fifty-four (54) federal government departments and agencies, representing a total of eighty-eight (88) departmental offices accept direct deposits and wire transfers.

The period of any resulting contract will be for three years from date of contract, with an irrevocable option to extend the period of the Contract by two (2) additional one (1) year period plus a six (6) months transition under the same terms and conditions.

2.2 There is a security requirement associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. Bidders should consult the Security Requirements for PWGSC Bid Solicitations - Information for PWGSC Contracting Officers (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31) document on the Departmental Standard Procurement Documents Web Site.

Bidders who currently do not meet the facility security clearance requirements and (or) personnel security clearance are advised to initiate the security clearance process immediately by requesting sponsorship

from the Contracting Authority. For any inquiries concerning any security requirements, bidders should contact CISD at 1-866-368-4646, or (613) 948-4176 in the National Capital Region (NCR), CISD Website: http://ssi-iss.tpsgc-pwgsc.gc.ca/.

3. Debriefings

After contract award, bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days of receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

1. Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2012-11-19), Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: sixty (60) days
Insert: one hundred twenty (120) calendar days.

1.1 SACC Manual Clauses

A7035T (2007-05-25), List of Proposed Subcontractors

2. Submission of Bids

Bids must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation. Bids transmitted to PWGSC by electronic mail will not be accepted.

Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

3. Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than ten (10) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all bidders. Enquiries not submitted in a form that can be distributed to all bidders may not be answered by Canada.

4. Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the bidders.

5. Basis for Canada's Ownership of Intellectual Property

Public Works and Government Services Canada has determined that any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, on the following grounds:

where the material developed or produced consists of material subject to copyright, with the exception of computer software and all documentation pertaining to that software.

PART 3 - BID PREPARATION INSTRUCTIONS

1. Bid Preparation Instructions

Canada requests that bidders provide their bid in separately bound sections as follows:

Section I: Technical Bid (4 hard copies);
Section II: Financial Bid (2 hard copies); and
Section III: Certifications and related documentation (1 hard copie).

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

Canada requests that bidders follow the format instructions described below in the preparation of their bid:

(a) use 8.5 x 11 inch (216 mm x 279 mm) paper; and
(b) use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process on Policy on Green Procurement.

To assist Canada in reaching its objectives, bidders should:

1) use paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and

2) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

Section I: Technical Bid

In their technical bid, bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Section II: Financial Bid

1.1 Bidders must submit their financial bid in Canadian funds and in accordance with the pricing schedule detailed in Attachment 1 to Part 3. The total amount of Applicable Taxes must be shown separately.

1.2 Bidders must submit their prices and rates FOB destination; Canadian customs duties and excise taxes included, as applicable; and Applicable Taxes excluded.

1.3 When preparing their financial bid, bidders should review the basis of payment in Annex B and clause 1.2, Financial Evaluation, of Part 4.

1.4 Bidders should include the following information in their financial bid:

1. Their legal name;
2. Their Procurement Business Number (PBN); and
3. The name of the contact person (including this person's mailing address, phone and facsimile numbers and email address) authorized by the Bidder to enter into communications with Canada with regards to:
   a. their bid; and
   b. any contract that may result from their bid.

1.5 SACC Manual Clauses

C3011T(2010-01-11), Exchange Rate Fluctuation

Section III: Certifications

Bidders should provide the certifications required under Part 5 and the related documentation in Section III of their bid.

ATTACHMENT 1 to PART 3
PRICING SCHEDULE

The Bidder should complete this pricing schedule and include it in its financial bid once completed. As a minimum, the Bidder must respond to this pricing schedule by including in its financial bid for each of the periods specified below its quoted firm all inclusive fee (in Cdn $) for each of the categories identified.

The inclusion of volumetric data in this document does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

The only categories of fees that may be proposed are:

A. EFT per Transaction Fee;
B. One-Time Departmental Office Setup Fee;
C. Monthly Departmental Online User Access Fee;
D. Collateral Charges on Transactions Equal or Greater than $50 M.

Note: All other costs to the bidder must be recovered in the above fees.

1.0 Calculation of Total Evaluated Price (TEP)

For evaluation purposes only, the Total Evaluated Price (TEP) will be the arithmetic sum of the following categories A, B, C and D as described below:
Any grey fields are for evaluation purposes only and should not be completed by the bidder.

A. EFT Transaction Fees:

Firm all-inclusive transaction fee for each direct deposit and wire transfer transaction included on the EFT daily EDI 821 electronic bank statement. This all-inclusive transaction fee must include all processing and reporting requirements.

Instructions

a) Bidders should clearly specify a Firm all-inclusive transaction Fee for each annual volume range and for each year in rows 1-3 of Tables A1 and A2 (columns B, D, F, H and J).

b) If a bidder wishes to offer a flat fee regardless of volume, it must enter the same fee for each volume range in Tables A1 and A2.

c) The Evaluation Team will use Table A3 to assist in the completion of the Summary of Charges – Total Evaluated Price (TEP) in Table E1. The annual weighted fee for EFT transactions will be calculated as: ((the arithmetic sum of the Weighted Volume Range Price Factors) * (the annual Forecasted EFT Direct Deposit Volumes)) + ((the arithmetic sum of the Weighted Volume Range Price Factors) * (the annual Forecasted EFT Wire Transfer Volumes)). **Table A3 is for evaluation purposes only and should not be completed by the bidder.**

Table A1 - Direct Deposit

EFT DIRECT DEPOSIT FIRM ALL INCLUSIVE TRANSACTION FEES												
		A	B	C	D	E	F	G	H	I	J	K
	Annual Volume Range	**Weighting Factor**	**Year 1 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*B)**	**Year 2 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*D)**	**Year 3 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*F)**	**Option Year 1 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*H)**	**Option Year 2 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*J)**
1	**1 – 5,000**	**.20**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
2	**5,000 – 10,000**	**.50**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
3	**10,001 +**	**.30**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
4	**Total Weighted Fee per Transaction (1 + 2 + 3)**			**$**		**$**		**$**		**$**		**$**

Table A2 - Wire Transfer

EFT WIRE TRANSFER FIRM ALL INCLUSIVE TRANSACTION FEES												
		A	B	C	D	E	F	G	H	I	J	K
	Annual Volume Range	**Weighting Factor**	**Year 1 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*B)**	**Year 2 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*D)**	**Year 3 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*F)**	**Option Year 1 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*H)**	**Option Year 2 Fees per Transaction Volume Range**	**Weighted Volume Range Price Factor (A*J)**
1	**1 – 15,000**	**.20**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
2	**15,000 – 30,000**	**.50**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
3	**30,001 +**	**.30**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**	**$**
4	**Total Weighted Fee per Transaction (1 + 2 + 3)**			**$**		**$**		**$**		**$**		**$**

Table A3 -Summary of Annual Weighted EFT Transaction Fees

Table A3 is for evaluation purposes only and should not be completed by the bidder.

	ANNUAL WEIGHTED EFT TRANSACTION FEE					
	Category	Year 1	Year 2	Year 3	Option Year 1	Option Year 2
1	Forecasted Annual Direct Deposit Volume	6,197	6,507	6,833	7,174	7,533
2	Total Weighted Fee per Transaction (input values from row 4 of Table A1)	**$**	**$**	**$**	**$**	**$**
3	**Annual Weighted Direct Deposit Fee** (rows 1 * 2)	**$**	**$**	**$**	**$**	**$**
4	Forecasted Annual Wire Transfer Volume	19,221	20,182	21,191	22,251	23,363
5	Total Weighted Fee per Transaction (input values from row 4 of Table A2)	**$**	**$**	**$**	**$**	**$**
6	**Annual Weighted Wire Transfer Fee** (rows 4 * 5)	**$**	**$**	**$**	**$**	**$**
7	**Annual Weighted EFT Transaction Fee** (rows 3 + 6)	**$**	**$**	**$**	**$**	**$**

B. Departmental Office Setup Fees:

One time charge to establish and maintain a departmental office with the capability of receiving EFT remittances, whether that departmental office involves an individual department or a division or programs within a particular department which the RG has deemed appropriate to setup with its own revenue receipt/reporting identity. These fees must include all administrative activities required to allow for this capability.

Instructions

a) Bidders should clearly specify a Firm all-inclusive departmental office setup fee for each contract year in row 2 of Table B1 (columns A, B, C, D, and E).

b) The total annual estimated setup fees will be calculated as: (the one-time all-inclusive setup fee) * (the estimated annual setup volumes). This calculation will be completed in row 3 of Table B1.

Table B1 -One-Time Firm All-Inclusive Departmental Office Setup Fees

ONE-TIME FIRM ALL-INCLUSIVE DEPARTMENTAL OFFICE SETUP FEES						
		A	**B**	**C**	**D**	**E**
		Year 1	**Year 2**	**Year 3**	**Option Year 1**	**Option Year 2**
1	**Estimated Annual Setup Volumes**	100	10	5	5	5
2	**One-Time All-Inclusive Setup Fee**	**$**	**$**	**$**	**$**	**$**
3	**Total Annual Estimated Setup Fees** (rows 1 * 2)	**$**	**$**	**$**	**$**	**$**

C. Departmental Online User Access Fees:

Monthly charge to establish and maintain departmental online user access to the Bidder's Online Reporting Tool. These fees would include all administrative activities required to allow for this capability.

Instructions

a) Bidders should clearly specify a per-user monthly firm all-inclusive access fee for each contract year in row 2 of Table C1 (columns A, B, C, D, and E).

b) The annual Firm all-inclusive access fee for Departmental Online User Access will be calculated as: (the per-user monthly firm all-inclusive access fee) * (the estimated departmental online user volumes) * (12 months). This calculation will be completed in row 4 of Table C1.

Table C1 -Monthly All-Inclusive Departmental Online User Access Fees

MONTHLY FIRM ALL-INCLUSIVE DEPARTMENTAL ONLINE USER ACCESS FEES						
		A	B	C	D	E
		Year 1	Year 2	Year 3	Option Year 1	Option Year 2
1	**Estimated Departmental Online User Volumes**	225	245	255	265	275
2	**Per-User Monthly Firm All-Inclusive Access Fee**	**$**	**$**	**$**	**$**	**$**
3	**Months**	**12**	**12**	**12**	**12**	**12**
4	**Annual Access Fee** (rows 1 * 2 * 3)	**$**	**$**	**$**	**$**	**$**

D. Collateral Charges on Transactions Greater than, or Equal to, $50 million

A firm basis point spread (bps) rate will be paid on all individual transactions received that are greater than, or equal to, $50 million. As the Contractor must transfer funds to the RG's account at the BoC on the same day the funds were received for all transfers received before 14:00 EDT, and next day for any funds received after 14:00 EDT, we do understand that additional collateral may need to be raised on days when large value transactions are received. For this reason, we are providing a method for the Contractor to charge for collateral costs on individual transactions received that are greater than, or equal to, $50 million.

This bps rate should be expressed as a whole number. For example, 8 basis points should be represented by the number 8.

Instructions

a) Bidders should clearly specify a Firm bps for each contract year in row 2 of Table D1 (columns A, B, C, D, and E).
b) The annual all-inclusive collateral charges on transactions greater than, or equal to, $50 million will be calculated as: (the Basis Point Spread (BPS)) * (the annual forecasted transfers greater than, or equal to, $50M)/ (the number of business days). This calculation will be completed in row 4 of Table D1.
    a. The basis point spread will be represented as follows in the formula: 8 basis points will be calculated as .0008 in decimal format for the purpose of calculating annual charges.
    b. The number of business days per year equals to 250.

Table D1 - All-inclusive collateral charges on transactions greater than, or equal to, $50 million

ALL-INCLUSIVE COLLATERAL CHARGES ON TRANSACTIONS GREATER THAN, OR EQUAL TO, $50 MILLION						
		A	B	C	D	E
		Year 1	**Year 2**	**Year 3**	**Option Year 1**	**Option Year 2**
1	**Forecasted Annual Value** (Sum of transaction ≥ $50 M)	**$4,079,000,000**	**$4,283,000,000**	**$4,497,000,000**	**$4,722,000,000**	**$4,958,000,000**
2	**Firm all-inclusive Basis Point Spread (BPS) on transactions greater than, or equal to $50 million**					
3	**Number of business days**	**250**	**250**	**250**	**250**	**250**
4	**Annual All-Inclusive Collateral Charge** $\frac{1 \times 2}{3}$	**$**	**$**	**$**	**$**	**$**

E. Summary of Charges - Total Evaluated Price (TEP) - FOR EVALUATION PURPOSES ONLY

The Total Evaluated Price (TEP) will be the arithmetic sum of the four categories A, B, C and D as described above.

Table E1 is for evaluation purposes only and should not be completed by the bidder.

Table E1 - TOTAL EVALUATED PRICE (TEP)

		1	2	3	4	5
		Contract Period Year 1	Contract Period Year 2	Contract Period Year 3	Option Year 1	Option Year 2
Item	Description	Annual Fees/charges	Annual Fees/charges	Annual Fees/charges	Annual Fees/charges	Annual Fees/charges
A	EFT Transaction Fees (Annual weighted fee from row 7 of Table A3)	$	$	$	$	$
B	Departmental Office Setup Fees (Annual Setup fee from row 3 of Table B1)					
C	Departmental Online User Access Fees (Annual Access fee from row 4 of Table C1)	$	$	$	$	$
D	Collateral Charges on transactions greater than, or equal to, $50 million (Annual all-inclusive charge from row 4 of Table D1)	$	$	$	$	$
Annual Evaluated Price =		$ (sum of col.1)	$ (sum of col.2)	$ (sum of col.3)	$ (sum of col.4)	$ (sum of col.5)
TOTAL EVALUATED PRICE (TEP) = (sum of the Annual Evaluated Prices of columns 1,2,3,4 and 5)					$_____	

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

1. Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical evaluation criteria.

(b) An evaluation team composed of representatives of Canada will evaluate the bids.

1.1 Technical Evaluation

1.1.1 Mandatory Technical Criteria

Refer to Attachment 1 to Part 4.

1.2 Financial Evaluation

1.2.1 The volumetric data included in the pricing schedule detailed in Attachment 1 to Part 3 are provided for bid evaluated price determination purposes only. They are not to be considered as a contract guarantee.

1.2.2 For bid evaluation and contractor(s) selection purposes only, the evaluated price of a bid will be determined in accordance with the Pricing Schedule detailed in Attachment 1 to Part 3.

2. Basis of Selection

2.1 Basis of Selection - Lowest Evaluated Price

A bid must comply with the requirements of the bid solicitation and meet all mandatory evaluation criteria to be declared responsive.

The responsive bid with the lowest evaluated price will be recommended for award of a contract.

ATTACHMENT 1 to PART 4
TECHNICAL CRITERIA

1.1.1 Mandatory Technical Criterion

The bid must meet the mandatory technical criterion specified below. The Bidder must provide the necessary documentation to support compliance with this requirement.

Bids which fail to meet the mandatory technical criterion will be declared non-responsive.

Mandatory Technical Criteria (MT)

For the purpose of the mandatory technical criterion specified below, the experience of the Bidder will be considered.

Number	Mandatory Technical Criterion	Bid Preparation Instructions
MT1	At solicitation's closing date, the Bidder must be a Canadian Payment Association (CPA) Large Value Transfer System (LVTS) participant.	The Bidder should furnish proof of CPA LVTS membership such as a membership certificate, membership number or letter of acceptance from the CPA. The Bidder should provide the necessary documentation to support compliance.

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications and related documentation to be awarded a contract. Canada will declare a bid non-responsive if the required certifications and related documentation are not completed and submitted as requested. Bidders should provide the required certifications and related documentation in Section III of their bid.

Compliance with the certifications bidders provide to Canada is subject to verification by Canada during the bid evaluation period (before award of a contract) and after award of a contract. The Contracting Authority will have the right to ask for additional information to verify bidders' compliance with the certifications before award of a contract. The bid will be declared non-responsive if any certification made by the Bidder is untrue, whether made knowingly or unknowingly. Failure to comply with the certifications, to provide the related documentation or to comply with the request of the Contracting Authority for additional information will also render the bid non-responsive.

1. Certifications Precedent to Contract Award

1.1 Code of Conduct and Certifications - Related Documentation

By submitting a bid, the Bidder certifies as per section 01 of Standard Instructions 2003, for himself and his affiliates, to be in compliance with the Code of Conduct and Certifications clause of the Standard instructions. The related documentation there in required will help Canada in confirming that the certifications are true.

1.2. Additional Certifications Precedent to Contract Award

The certifications included in Attachment 1 to Part 5, Certifications Precedent to Contract Award, should be completed and submitted with the bid, but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will so inform the Bidder and provide the Bidder with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within that time period will render the bid non-responsive.

ATTACHMENT 1 to PART 5
CERTIFICATIONS PRECEDENT TO CONTRACT AWARD

1.1 Federal Contractors Program

1.1.1 Federal Contractors Program - $200,000 or more

1. The Federal Contractors Program (FCP) requires that some suppliers, including a supplier who is a member of a joint venture, bidding for federal government contracts, valued at $200,000 or more (including Applicable Taxes), make a formal commitment to implement employment equity. This is a condition precedent to contract award. If the Bidder is subject to the FCP or, if the Bidder is a joint venture and if any of the members of the joint venture is subject to the FCP, evidence of the commitment made by the Bidder or by each member of the joint venture who is subject to the FCP must be provided by the Bidder before the award of any contract resulting from the bid solicitation.

   Suppliers who have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive government contracts over the threshold for solicitation of bids as set out in the *Government Contracts Regulations*. Suppliers may be declared ineligible contractors either, as a result of a finding of non-compliance by HRSDC, or, following their voluntary withdrawal from the FCP for a reason other than the reduction of their workforce to less than 100 employees. Any bids from ineligible contractors, including a bid from a joint venture that has a member who is an ineligible contractor, will be declared non-responsive.

2. The Bidder or, if the Bidder is a joint venture, any of the members of the joint venture who does not fall within the exceptions enumerated in 3.a or b below or does not have a valid certificate number confirming its adherence to the FCP must fax (819-953- 8768) a copy of the signed form LAB 1168, Certificate of Commitment to Implement Employment Equity, to the Labour Branch of HRSDC.

3. The Bidder or, if the Bidder is a joint venture, the member of the joint venture certifies its status with the FCP, as follows:

   The Bidder or the member of the joint venture

   a. ( ) is not subject to the FCP, having a workforce of less than 100 permanent full-time, permanent part-time and/or temporary employees having worked 12 weeks or more in Canada;

   b. ( ) is not subject to the FCP, being a regulated employer under the Employment Equity Act, S.C. 1995, c. 44;

   c. ( ) is subject to the requirements of the FCP, having a workforce of 100 or more permanent full-time, permanent part-time and/or temporary employees having worked 12 weeks or more in Canada, but has not previously obtained a certificate number from HRSDC (having not bid on requirements of $200,000 (including Applicable Taxes) or more), in which case a duly signed certificate of commitment is attached;

   d. ( ) is subject to the FCP, has not been declared an ineligible contractor by HRSDC, and has a valid certificate number as follows: _____ .

Further information on the FCP is available on the HRSDC Web site.

1.2 Former Public Servants Certification

Contracts with former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny and reflect fairness in spending public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below.

Definitions

For the purposes of this clause,

"former public servant" is any former member of a department as defined in the *Financial Administration Act, R.S. , 1985, c. F-11*, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

a) an individual;
b) an individual who has incorporated;
c) a partnership made of former public servants; or
d) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means, a pension or annual allowance paid under the *Public Service Superannuation Act (PSSA)* , R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act* , R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act* , R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act* , 1970, c. D-3, the *Royal Canadian Mounted Police Continuation Act* , 1970, c. R-10, and the Royal Canadian Mounted Police Superannuation Act , R.S., 1985, c. R-11, *the Members of Parliament Retiring Allowances Act* , R.S., 1985, c. M-5, and that portion of pension payable to the*Canada Pension Plan Act* , R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

The Bidder must provide an answer to the following question:

As per the above definitions, is the Bidder a FPS in receipt of a pension? **YES ( ) NO ( )**; and

if the answer is YES, the Bidder must provide the following information for all FPS in receipt of a pension, as applicable:

a) name of former public servant; and
b) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Reduction Program

The Bidder must provide an answer to the following question:

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of a work force reduction program? **YES ( ) NO ( )**; and

if the answer is YES, the Bidder must provide the following information:

a) name of former public servant;
b) conditions of the lump sum payment incentive;
c) date of termination of employment;
d) amount of lump sum payment;
e) rate of pay on which lump sum payment is based;
f) period of lump sum payment including start date, end date and number of weeks; and
g) number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

Certification

By submitting a bid, the Bidder certifies that the information submitted by the Bidder in response to the above requirements is accurate and complete.

1.3 Canadian Content Certification

1.3.1. SACC Manual clause A3050T, Canadian Content Definition.

1.3.2 Canadian Content Certification

This procurement is limited to Canadian services.

The Bidder certifies that:

( ) the service offered is a Canadian service as defined in paragraph 2 of clause A3050T.

1.4 CPA LVTS Participant

Should it be awarded a contract as a result of the bid soliciation, the Bidder certifies that its status and membership as a Canadian Payment Association (CPA) Large Value Transfer System (LVTS) participant will be maintained during the period of the Contract and any exercised options including any resulting transition period.

PART 6 - SECURITY AND FINANCIAL REQUIREMENTS

1. Before award of a contract, the following conditions must be met:

   (a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

   (b) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirement as indicated in part 7 - Resulting Contract Clauses;

   (c) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites or;

   (d) the Bidder's proposed location of work performance or document safeguarding must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses;

   (e) the Bidder must provide the address(es) of proposed location(s) of work performance or document safeguarding.

2. Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

3. For additional information on security requirements, bidders should consult the "Security Requirements for PWGS Bid Solicitations - Instructions for Bidders" (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31) document on the Departmental Standard Procurement Documents Website

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

1. Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work in Annex A.

1.1 Optional Goods or Services, or both

The Contractor grants to Canada the irrevocable option to acquire the goods, services or both described at Annex A of the Contract under the same conditions and at the prices and/or rates stated in the Contract. The option may only be exercised by the Contracting Authority and will be evidenced, for administrative purposes only, through a contract amendment.

The Contracting Authority may exercise the option at any time before the expiry of the Contract by sending a written notice to the Contractor.

1.2 Destination of Services

Public Workds and Government Services Canada
National Capital Area (Gatineau)
Phase III, Place du Portage
11 Laurier Street
Gatineau, Quebec K1A 0S5
Canada

2. Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines /standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

2.1 General Conditions

2035 (2013-03-21), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

2.2 Supplemental General Conditions

4008 (2008-12-12), Personal Information, apply to and form part of the Contract.

3. Security Requirement

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B issued by the Canadian Industrial Security Directorate, Public Works and Government Services Canada.

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

3. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be per-formed at the level of PROTECTED B.

4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

5. The Contractor/Offeror must comply with the provisions of the:

(a) Security Requirements Check List, Annex C and Attachment 1 to Annex C - IT Security Requirements;
(b) Industrial Security Manual (Latest Edition)

4. Term of Contract

4.1 Period of the Contract

The period of the Contract is for three years from date of Contract award.

4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two (2) additional one (1) year period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least thirty (30) calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

4.3 Option to Extend - Transition Period

The Contractor acknowledges that the nature of the services provided under the Contract requires continuity and that a transition period may be required at the end of the Contract. The Contractor agrees that Canada may, at its discretion, extend the Contract by a period of 6 months under the same conditions to ensure the required transition. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

The Contracting Authority will advise the Contractor of the extension by sending a written notice to the Contractor at least 30 calendar days before the contract expiry date. The extension will be evidenced for administrative purposes only, through a contract amendment.

4.4 Termination on Thirty Days Notice

1. Canada reserves the right to terminate the Contract at any time in whole or in part by giving thirty (30) calendar days written notice to the Contractor.

2. In the event of such termination, Canada will only pay for costs incurred for services rendered and accepted by Canada up to the date of the termination. Despite any other provision of the Contract, there will be no other costs that will be paid to the Contractor as a result of the termination.

5. Authorities

5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name*:* Jocelyne C Gagnon
Title: Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Directorate: Business Management and Consulting Services Division
Address:11 Laurier Street
Portage III, 10C1
Ottawa, Ontario, K1A 0S5

Telephone: (819) 956-0575
Facsimile: (819) 956-2675
E-mail address: jocelyne.c.gagnon@tpsgc-pwgsc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

5.2 Project Authority

The Project Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone: ___- ___- ___
Facsimile: ___- ___- ___
E-mail address: _____

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

5.3 Contractor's Representative (will be identified at contract award)

The Contractor’s representative is:

6. Payment

6.1 Basis of Payment

6.1.1 Firm Unit Price

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid the firm all-inclusive fee as specified in Annex B, Basis of payment. Customs duties are included and Applicable Taxes are extra.

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

The Contractor must notify the Contracting Authority in writing when the total estimated cost on p.1 of the contract is 75 percent committed. Canada's total liability to the Contractor under the Contract must not exceed the total estimated cost on page 1.

The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority.

6.2 Method of Payment

6.2.1 Monthly Payments

SACC Manual Clause H1008C (2008-05-12), Monthly Payment

6.3 SACC Manual Clauses

A9117C (2007-11-30), T1204 - Direct Request by Customer Department
C2000C (2007-11-30), Taxes - Foreign-based Contractor

6.4 Discretionary Audit

C0705C (2010-01-11), Discretionary Audit

7. Invoicing Instructions

The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.

Each invoice must be supported by:

(a) a copy of the release document and any other documents as specified in the Contract; and
(b) a copy of the invoices, receipts, vouchers for all direct expenses.

Invoices must be distributed as follows:

(a) The original and one (1) copy must be forwarded to the address shown on page 1 of the Contract for certification and payment.
(b) One (1) copy must be forwarded to the Contracting Authority identified under the section entitled "Authorities" of the Contract.

8. Certifications

8.1 Compliance

Compliance with the certifications and related documentation provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the term of the Contract. If the Contractor does not comply with any certification, provide the related documentation or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

8.2 SACC Manual Clauses

A3050T (2010-01-11), Canadian Content Definition
A3060C (2008-05-12), Canadian Content Certification

9. Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

10. Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

(a) the Articles of Agreement;
(b) the supplemental general conditions 4008 (2008-12-12);
(c) the general conditions 2035 (2013-03-21), General Conditions - Higher Complexity - Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirements Check List; and
(g) the Contractor's bid dated _____

11. Foreign Nationals

11.1 SACC Manual clause A2001C (2006-06-16), Foreign Nationals (Foreign Contractor)

11.2 SACC Manual clause A2000C (2006-06-16), Foreign Nationals (Canadian Contractor)

11.3 SACC Manual clause A9122C (2008-05-12), Protection and Security of Data Stored in Database

12. Insurance

SACC Manual clause G1005C (*2008-05-12*) Insurance

ANNEX A
STATEMENT OF WORK

1.0 OVERVIEW

1.1 Introduction and Background

As the Receiver General for Canada (RG), the Minister of Public Works and Government Services Canada (PWGSC) manages the operations of the federal treasury, including the receipt and payment of federal money into and out of the Consolidated Revenue Fund (CRF). PWGSC consolidates the management of the government's payments and revenue collection so as to achieve the most competitive rates for services available from Canada's financial institutions (FIs).

Although the RG collects remittances through many arrangements, the requirements described within this Statement of Work (SOW) are only for Electronic Funds Transfer (EFT) services and are not to replace any other form of remittances made to the RG, such as cash; cheques; credit or debit cards; pre-authorized debits; or paper or electronic bill payments for which the RG has separate Contracts/arrangements.

Currently, fifty-four (54) federal government departments and agencies, representing a total of eighty-eight (88) departmental offices accept direct deposits and wire transfers. Direct deposit and wire transfer payments for the period between April 1, 2011 and March 31, 2012, amounted to approximately $2.4 billion and $14,4 billion respectively.

Please note that some large value incoming wire transfers have been excluded from this arrangement and as such are not included in the estimates and volumes provided. The transfers excluded from this arrangement are monthly transfers between the Canada Pension Plan Investment Board (CPPIB) and Human Resources and Skills Development Canada (HRSDC).

1.2 Objective

A formal arrangement with a single service provider, hereafter referred to as the Contractor, is sought for incoming Electronic Funds Transfers (EFT). This service is to cover payments made to the government by direct deposit and wire transfer that are denominated in Canadian dollars.

1.3 Definitions

Please refer to *Annex A, Appendix 1 - Definitions* for the definitions that are used throughout this document.

1.4 Current Arrangements

Currently, direct deposits and wire transfers are received by the RG through an arrangement with a single Canadian FI.

1.5 Statistical Information

Historical value and volume statistics for direct deposit and wire transfer remittances are provided in *Annex A, Appendix 6 - Historical EFT Activity*.

In addition, value and volume forecasts are provided in *Annex A, Appendix 7 - Banking Values and Volumes Remittances Forecast for 2014 To 2018*. Although great care has been made to accurately predict the future volumes, there is no guarantee that these predictions will materialize. All statistics are estimated in good faith for informational purposes only and MUST not be construed to represent the amount that the Government of Canada will receive through the EFT service.

2.0 DETAILED SERVICE REQUIREMENTS

2.1 General Business Requirements

The Contractor MUST provide the following services:

i. Acceptance of direct deposit and wire transfer payments made in Canadian dollars, originating from within and outside of Canada.

ii. Ensuring that all "on-us" transactions (transactions in which the customer's financial institution and the Contractor are the same institution) are processed in accordance with the Canadian Payments Association (CPA) rules governing direct deposits and wire transfer payments (i.e. CPA F Rules for Direct Deposits, and CPA LVTS rules for wire transfers) even if they are not technically subject to these rules. This is to ensure that processing of each transaction is not treated differently depending at which FI the customer initiates the transaction.

iii. Same business day remittance of value to the RG's account at the Bank of Canada (BoC) in accordance with the "Settlement" section (2.8) on any remittances received by 14:00 EDT. Any remittances received after 14:00 EDT MUST be transferred the next business day.

iv. Reporting of remittance information, through an online reporting tool, to the appropriate departmental offices and the RG in accordance with the "Online Reporting" section (3.2).

v. Next business day electronic reporting of account activity (bank statement) to the RG in accordance with the "Reporting to the Receiver General for Canada" section (3.1).

vi. Response to enquiries from the RG relating to EFT transactions in accordance with the "Traces and Enquiries" section (2.10).

2.2 Opening of Concentrator Account

The Contractor MUST open a Concentrator Account in Canada, in the name of "The Receiver General for Canada - EFT Remittances".

2.3 Opening of Sub-Accounts

The Contractor must open sub-accounts for each departmental office to facilitate the required reporting as stated in the "Reporting Requirements" section (3.0). Sub-account balances MUST clear daily to the Concentrator Account. This means that the presentation date (the date that a transaction was received by the Contractor) should always be the same as the concentrator date (the date that the funds were transferred to the concentrator account), except under exceptional circumstances.

2.4 Posting EFTs to the Concentrator Account/Sub-Accounts

i. The Contractor MUST post each individual EFT remittance received to the appropriate sub-account within one (1) hour of receipt.

ii. The Contractor must clear each sub-account daily to the concentrator account with a concentrator date equal to the presentation date of each transaction. This means that, regardless of whether the funds are transferred same or next day to the BoC, the presentation date and concentrator date should still be the same.

iii. The RG will assign a unique authorization number to each departmental office that wishes to participate in the EFT Service. The Contractor MUST report this authorization number in the electronic bank statement for each account posting (other than the transfers to the BoC). In addition, the Contractor is encouraged to provide a unique EFT reference number in the electronic bank statement for each account posting that is also in the remittance information reported to the appropriate department to facilitate reconciliation.

2.5 Contractor Initiated Adjustments

The Contractor MUST post all adjustments separately to the appropriate sub-account. The original incorrect entry MUST be reversed and a correct entry MUST be made. The Contractor, on the same day as the account posting, MUST forward documentation to substantiate the adjustment to the RG and also to the appropriate departmental office.

2.6 Remitter Instruction Advice

The Contractor MUST provide advice on the drafting of EFT remitter instructions that will facilitate complete and accurate reporting of the remittance information that the departmental office requires to identify the payor, the intended departmental office payee, and the purpose of the payment. These instructions must clearly indicate the messaging that must accompany each transaction to ensure that all beneficiary and intermediary bank fees are absorbed by the payor. The instructions must also contain information required by the payor to initiate transactions from within and outside of Canada.

2.7 Charges

As per section 2.6, all remitter instructions will indicate that all beneficiary and intermediary bank fees are paid by the payor. As such, no EFT charges are to be deducted from the original amount by the Contractor.

2.8 Settlement

The Contractor MUST transfer funds to the RG's account at the BoC on the same day the funds were received for all transfers received before 14:00 EDT. Any funds received after 14:00 EDT MUST be transferred to the RG's account at the BoC the next business day.

The day on which the funds are transferred to the BoC will be known as the settlement date. Float interest will be applicable on next day transfers and will be calculated in accordance with the "Float" section (2.9).

The Contractor must initiate and send to the BoC before 15:00 EDT a LVTS payment message MT103 in favour of the RG containing any same day balances received by 14:00 EDT, as well as all outstanding previous day balances. The required MT103 formatting can be found in *Annex A, Appendix 5 - Bank of Canada LVTS Formatting Requirements*. Please note that same day and previous day balances must be sent in separate LVTS MT103 payment messages.

2.9 Float

The Contractor MUST pay float interest to the RG on any funds where the settlement date is later than the presentation date. This float interest will be calculated in accordance with the rate specified in the Memorandum of Understanding (MOU) negotiated between the direct clearing FIs and the Government of Canada. This rate is currently calculated as the bank rate (as per the Bank of Canada) less one quarter of one percent (0.25%), although the rate is subject to change.

In the event an error is made on the part of the RG or the Contractor, or a situation involving exceptional circumstances occurs which causes a negative float impact to the Contractor or the RG beyond the interest rate stipulated in the MOU, a higher rate of interest may be paid up to, but not exceeding, the actual financial impairment incurred. Any such occurrence MUST be reviewed by the RG.

2.10 Traces and Enquiries

The Contractor MUST make every effort to resolve any enquiries and/or to provide clarification of a remittance within five (5) business days when requested by the RG. Upon failure to resolve an enquiry within five (5) business days, the RG may escalate the enquiry within the Contractor's organization. All trace or enquiry requests from the RG will include an Original Enquiry Number; this number MUST be referenced in all responses.

3.0 REPORTING REQUIREMENTS

3.1 Reporting to the Receiver General for Canada

The Contractor MUST provide a daily EDI 821 electronic bank statement of the concentrator account to the RG by 08:00 EDT on the first business day following the concentrator date. Within the EDI 821 electronic bank statement, the Contractor must:

i. Report each wire transfer and direct deposit transaction individually.

ii. Report each adjustment individually on the EDI 821 bank statement.

iii. Ensure that the REF 02 segment is populated with the RG authorization number assigned to the sub-account.

iv. Ensure that appropriate financial transaction codes are provided for all incoming direct deposit transactions, incoming wire transfer transactions, and adjustments in the FIR01 segment. Although we do not require transfers between the sub-accounts and the concentrator account or between the concentrator account and the BoC to be reported on the EDI 821 bank statement, should the Contractor decide to include these we would require these types of transfers to have their own separate transaction codes in the FIR01 segment so that we may separate actual transactions from the movement of funds.

v. Ensure that the BGN03 segment is populated with the date that the funds were posted to the concentrator account (concentrator date)

vi. Ensure that the FIR07 segment is populated with the date that each transaction was received by the Contractor (presentation date).

The current protocol and mappings for electronic reporting of bank statements are provided in *Annex A, Appendices 2, 3 and 4*.

3.2 Online Reporting

The Contractor MUST provide secure online access in "Read Only Mode" of all account activities including direct deposit transactions; wire transfer transactions; adjustments; and transfers to the concentrator account and the BoC. Each departmental office should only have access to the specific transactions associated with their authorization number, while the RG should have broader access through which it can view transactions for all authorization numbers as well as the concentrator account. The Contractor must provide the following services related to online reporting:

i. Make remittance information for direct deposit and wire transfer transactions available within one (1) hour of receipt by the Contractor. In certain situations, upon request by the RG, the Contractor must also be able to provide to the RG and appropriate departmental office real-time reporting of specific time-sensitive transactions.

ii. Restrict access to only authorized departmental office employees who have been granted "Read Only" privileges.

iii. Maintain availability of data on the online reporting tool for a minimum of six (6) months.

iv. Have the capability to allow departments to download the data on to their own systems using spreadsheet software.

v. Offer bilingual help desk support in accordance with the "Help Desk Support" section (5.2) for the set-up of new users and for troubleshooting purposes.

vi. For adjustments, information regarding the reason for the adjustment be made available through the online reporting tool.

vii. For wire transfers, all remittance information contained in the payment message received by the Contractor must be made available through the online reporting tool.

viii. For direct deposits, the Contractor must provide at a minimum the following remittance information contained in the CPA Standard 005 Logical Record "C" (if it is received from the remitter/remitting FI):

a. Originator Short Name (Data Element 11) or, where available, the Originator Long Name (Data Element 13);
b. Transaction Type (Data Element 04);
c. Originator's Sundry Information (Data Element 18); and
d. Amount (Data Element 05)

4.0 DEVELOPMENT AND IMPLEMENTATION OF THE EFT REMITTANCE SERVICE

4.1 Implementation of Service

Implementation activities must begin within 5 business days after date of contract award. These activities must include:

i. Within two (2) weeks of contract award (unless otherwise mutually agreed), the Contractor MUST brief the RG on the remittance service including best practices and respond to any questions.

ii. Within two (2) weeks of Contract award, review the EFT Setup Forms and identify what additional information the Contractor requires.

iii. Within two (2) weeks of contract award, provide a list of contacts (name, telephone number, e-mail address, fax number, and/or mailing address, where applicable) of the team leader, account manager and project manager to handle the issues associated with the administration of this Contract, as well as the second and third level escalation contacts and maximum turnaround times that can be expected. The Contractor's list of contacts of authorized personnel must include contacts for daily operations, security access issues, system/technical support for transition period and ongoing operations; and the delivery of the RG monthly invoice for services rendered.

iv. Within two (2) months of contract award (unless otherwise mutually agreed), the Contractor must implement existing EFT participating departmental offices.

v. Comply with the electronic configuration and testing requirement stipulated in *Annex A, Appendix 2 - Current Protocol for Electronic Reporting of Bank Statements*.

vi. Availability to test electronic files and reporting requirements in a test environment.

vii. Once approved by the RG, moving the electronic transmission into production.

viii. Liaising with the BoC to finalize settlement arrangements.

ix. Any other requirements as per the SOW.

x. Be fully operational for EFT services as stated in this SOW within a maximum of two (2) months from the date of Contract award, unless otherwise agreed to by the RG.

4.2 Implementation of New Departmental Offices

The Contractor MUST provide departmental offices with EFT Remittance Services on an as required basis and only upon receipt of an authorized EFT Request Form. Although this form is subject to change, a sample version of this form is provided in *Annex A, Appendix 8 - EFT Request Form*.

Any additional service or deletion of service requested by a department will also require an authorized EFT Request Form.

A department will make an official request to setup or amend a departmental office by preparing an EFT Request Form and forwarding it to the RG. The RG will then forward the form to the Contractor. All parties will extract their required information from the form and insert their identifiers (such as the RG Authorization #, Concentrator Account #, and sub-account #). Once all required identifiers have been received, the RG will return the approved Form to the appropriate department.

Upon receipt of an approved EFT Request Form, the Contractor MUST:

i. Extract any Contractor required information from the form;

ii. Complete the form by inserting any required identifiers such as a sub-account number;

iii. Return the form to the RG within three (3) business days of receipt;

iv. Be prepared to implement new or amended department office EFT services within two (2) weeks of receipt of a form (unless otherwise mutually agreed in writing);

v. Provide support if required in the testing and implementation of new or amended department EFT services;

vi. Provide ongoing support as required. This may include support during testing of new remitters for large dollar transactions.

The Contractor must not commence work until a EFT Request Form has been authorized by the Project Authority. The Contractor acknowledges that work performed before a EFT Request Form has been authorized will be done at the Contractor's own risk and expense;

4.3 Documentation and Training

The Contractor MUST provide the RG and departmental offices with bilingual, complete and current documentation (such as operator manuals) and training (such as ongoing help desk support) on the online reporting tool provided by the Contractor.

The RG will be responsible for the development of an EFT Service Terms of Engagement. This Terms of Engagement will provide departments with information such as:

- An overview of the EFT Service;
- A description of the direct deposit and wire transfer process;
- A description of the set-up process;
- Samples of remitter instructions;
- Help desk information such as set-up and problem resolution.

The Contractor MUST provide assistance to the RG in the development of this Terms of Engagement guide that may include recommendations and review of its content.

4.4 Phase-out (Transition Period) Provisions

The Contractor MUST, at the end of the operational phase of the Contract or upon notification by the Contracting Authority of our intent to terminate the Contract, continue to provide the same level of service on a reduced volume basis, under the same terms, conditions and pricing as stipulated in the Contract for a period not exceeding 6 months to clear transactions. The total contract period includes the operational phase and does not include phase-out (transition) period.

The Contractor further agrees that, if required by the Project Authority at the end of the phase-out (transition) period, the Contractor must provide the Project Authority with an electronic data file containing all of the information collected during the Contract period.

The Contractor further agrees to assist in ensuring a smooth transition to any new Contractor at the end of this contract with no break in service and with minimal disruption to government processes and operations.

5.0 OTHER REQUIREMENTS

5.1 Foreign Currency Transactions

This service has been designed specifically for the acceptance and processing of EFT remittances made in Canadian dollars only. The information provided by departments to remitters will emphasize this requirement. However, in the event that remitters do remit in foreign currencies, the Contractor MUST reject the transactions and inform the RG.

5.2 Help Desk Support

Help desk support in both official languages from Monday to Friday between the hours of 08:30 and 17:00 EDT MUST be provided by the Contractor on all business days.

The Contractor MUST provide telephone access for their help desk via a toll free number, in addition to email.

To assist the RG in reconciling the concentrator account, the Contractor MUST provide the phone numbers of persons who will assist in resolving problems.

The Contractor MUST respond directly to the departmental offices for any technical difficulties regarding the online reporting tool.

5.3 Security and Privacy

The Contractor MUST ensure compliance with the Information Technology Security Requirements identified in *Annex C and Attachment 1 to Annex C – IT Security Requirements*.

5.4 Contingency and Disaster Recovery

As outlined in *Annex C and Attachment 1 to Annex C – IT Security Requirements* , the Contractor MUST have a formal Contingency and Disaster Recovery Plan in place, in the event of power shortage, fire, labour disruption or any other situation that could lead to a disruption in provision of this service. In any such situation, the Contractor MUST use its best efforts to continue normal communications and reporting between it, the RG, and departmental offices by alternate means that are mutually agreed upon between the parties.

5.5 Periodic Threat and Risk Assessments

Upon the Project Authority's request, the Contractor MUST provide information to assist Canada in the preparation of a Statement of Sensitivity and Threat and Risk Assessment pertinent to the EFT services provided.

5.6 Canadian Payment Association (CPA)

The Contractor must be a Canadian Payment Association (CPA) Large Value Transfer system (LVTS) participant. The Bidder must maintain its status during the period of the Contract and any exercised options including any resulting transition period.

5.7 Language

The Contractor MUST be capable of providing services in both official languages of Canada: English and French. Personnel providing training (Help Desk) MUST provide bilingual, English and French services; however, documentation such as input to Terms of Engagements, rules, regulations, promotional material, can be provided in English and when available, in French.

Where the Project Authority finds the French versions of any materials listed to be unacceptable, the RG reserves the right to have its respective English versions re-translated at its own expense solely for departmental office use.

The Official Languages Act and Treasury Board Secretariat (TBS) policies and publications pertaining to this act can be viewed by accessing the following websites:
Http://laws-lois.justice.gc.ca/eng/acts/O-3.01
Http://www.tbs-sct.gc.ca/pol/index-eng.aspx

5.8 Changing of Payment Standards during Contract

As outlined in the CPA 2011 Annual Review, the CPA Board of Directors has agreed to establish ISO 20022 as the future direction for standards in Canada. The intention is to replace all of the standards used for payments that clear and settle through the CPA (including AFT Standard 005, SWIFT and LVTS) with ISO 20022. It is the intention of the RG to be an early adopter of this new standard. Should ISO 20022 be implemented during the life of this contract, and upon request by the RG, the Contractor MUST accept and send AFT, SWIFT and LVTS files in this new format.

Should the CPA decide to update the CPA Standard 005 to be able to provide enhanced remittance data as an intermediary step or an alternative to the establishment of ISO 20022, the Contractor MUST also remain compliant with the new standard.

5.9 Future Business Requirements

The manner in which the RG conducts business is subject to change over time as new delivery channels and improved technologies are developed. The financial service sector is leading similar changes, including introducing new collection services that are more timely, cost effective and convenient. The public is demanding these services and expectations are reinforced by the increasing awareness of what technology should enable.

The Project Authority may request from the Contractor or the Contractor may present to the Project Authority innovative approaches to technologies and services throughout the contract term and any optional years to improve customer service and/or decrease costs.

Any of these new services that are approved will only be implemented by means of a formal signed amendment to the Contract. The RG does not waive its right to go to competitive tender for new services. These new services may include but are not limited to the following:

- Services to accept and process additional types of EFT remittances;
- New technologies for EFT-based services as well as new methods of remittance reporting; and
- Services to standardize processes among federal departments or make changes that will reduce costs, improve efficiency, and quality of services provided.

ANNEX A, APPENDIX 1

DEFINITIONS

The following definitions are applicable to this SOW and may have different meanings in other contexts.

Authorization Number	Eight-digit number assigned by the RG to a Departmental Office, which has been authorized to accept EFT remittances.
Business Day	Any day from Monday to Friday excluding national holidays as specified by CPA definitions. Regional and civic holidays are considered to be business days.
Customers/Remitters	Person or organization making EFT remittances to Departmental Offices.
Concentrator Account	Account established in the name of the "Receiver General for Canada - EFT Remittances", specifically for the deposit of federal EFT remittances.
Concentrator Date	Date the RG receives value in the Concentrator Account.
Departmental Office	Federal government departmental office that has been authorized and set up by the RG to accept EFT remittances. Also referred to as the payee or beneficiary. A departmental office can be either a federal department as a whole, or a specific division or program within a department.
Direct Deposit	Deposit of funds directly into a bank account as a form of payment. Common uses for direct deposit include pay cheques and tax refunds.
EFT	Electronic Funds Transfers including Direct Deposit (DD) and Wire Transfer (WT) remittances.
Float	Value of Government of Canada receipts in transit between the Contractor and the Bank of Canada.
LVTS	A real-time payment transfer system that is owned and operated by the Canadian Payments Association to process large value payments and the electronic exchange of payment messages between LVTS participants.
Presentation Date	Date that a direct deposit or wire transaction is received by the Contractor.
Next Day Value	When the Settlement Date is one business day after the Presentation Date.
Payor	Originator of a Direct Deposit or Wire Transfer transaction.
Settlement Date	Date the RG receives value at the Bank of Canada.
Same Day Value	When the Settlement Date is the same as the Presentation Date.
Sub-Accounts	Accounts established in the name of the Receiver General that clear daily to the Concentrator Account. Sub-Accounts are used to assist in associating each transaction to the appropriate departmental office.

ANNEX A, APPENDIX 2

CURRENT PROTOCOL FOR ELECTRONIC REPORTING OF BANK STATEMENTS

The current protocol for electronic reporting of bank statements is via EDI ANSI X12 standard formats, as follows:

1. Transaction Sets

The following EDI Transaction Sets are exchanged between the parties:

a. ANSI X12 Envelope Specifications (hereinafter called "Envelop");
b. ANSI X12 821 Financial Information Reporting (hereinafter called "821");
c. ANSI X12 997 Functional Acknowledgement (hereinafter called "997").

The Envelope and 821 mappings are attached as Appendix 3 and 4 of Annex A.

2. Data Elements for 821s

821s currently MUST include the following data elements:

a. Financial Institution's Number as assigned by the Canadian Payments Association;
b. Transit Number of the branch where the Concentrator Account is located;
c. The Concentrator Account number being reported on;
d. Transaction Code (Type):

i. As a minimum, separate codes are required for authorized transactions as follows:
- Direct Deposits (DDs);
- bank initiated adjustments associated with DDs;
- wire deposits (WTs);
- bank initiated adjustments associated with WTs;
- transactions associated with transfers to the Bank of Canada or transfers between the sub-account and concentrator account.

ii. Unauthorized Postings

Action MUST be taken to stop unauthorized postings. Although the following transaction types are unauthorized for this Statement of Work, should they occur, as a minimum separate transaction codes are required for:

- manual over the counter deposits;
- bank initiated adjustments associated with manual over the counter deposits;
- returned items associated with manual over the counter deposits;
- electronic card deposits;
- bank initiated adjustments associated with electronic card deposits;
- returned items associated with electronic card deposits; and
- EDI 820/823 initiated deposits;
- bank initiated adjustments associated with EDI 820/823 initiated deposits;
- when appropriate (finality of payment is not requested and electronic charge backs are requested by the departmental office), returned items associated with EDI 820/823 initiated deposits;
- preauthorized debit (PAD) deposits;
- bank initiated adjustments associated with PAD deposits;
- returned items associated with PAD deposit.

e. Transaction concentrator date;

f. Transaction amount; and
g. RR, ZZ, PQ, IT, IX, VR, DE Reference Numbers as specified in Appendix 4 of Annex A.

3. Configuration and Test Period

Currently the RG requires contractors to:

a. Provide at least six (6) weeks prior to the Implementation Date, all mailbox and other pertinent information for system configuration.

b. Provide at least six (6) weeks prior to the Implementation Date, the list of mnemonic codes (along with their meanings) to be used as transaction codes (types).

c. Provide to the RG's test mailbox, a transmission of:

i. General 821 test data (which has been fabricated, and agreed to with the RG) at least four (4) weeks prior to the Implementation Date and as requested by the RG thereafter; and

ii. Real ($0) 821 data for the Concentrator Account on a daily basis, starting at least three (3) weeks prior to the Implementation Date and as requested by the RG thereafter.

4. Reporting process upon Implementation

Currently, the RG requires contractors to:

a. Adhere to the RG Test Plan and Release Procedures unless otherwise mutually agreed. The RG Test Plans and Release Procedures will be provided upon request.

b. Forward each banking day, in clear text, an 821 of the Concentrator Account to the RG's electronic production mailbox by no later than 8:00 a.m. Eastern Standard Time (EST), on the first banking day following the concentrator date.

c. Accept either a positive or negative 997 from the RG in response to each 821 transmitted by the contractor, taking follow-up action should the contractor not receive a 997 following each transmission. Follow-up action MUST take place by 10:00 a.m. EST, on the same day of each 821 transmission. Follow-up action MUST consist of a telephone call to the RG.

d. Upon receipt (ISA09 and ISA10 of the ANSI X1 2 envelope) of a negative 997, correct the 821 and retransmit within 2 hours from the time of such receipt.

e. In the event of inability to report as above, upon request by the RG, provide, in lieu of an 821, either a hard copy or alternate electronic form of the data elements listed in section 2 of Appendix 2 above. The foregoing medium MUST be mutually agreed.

f. Forward each banking day to the RG a copy of supporting documentation for any postings to the Concentrator Account not covered by this Statement of Work, to be received the same day as the 821.

5. Sender Pays Transmission Costs

The Receiver General requires contractors to pay all costs associated with the transmission of 821s. This includes sending to the Receiver General Mailbox, and receiving from the Receiver General Mailbox.

ANNEX A, APPENDIX 3

821/152 Envelope Specifications

821/152 Envelope Specifications

VERSION 003010

Receiver General

Release 3.02

Receiver General Envelope Specifications

Interchange Control Version Number 00200

SEG.ID	Name	Required	Loop
ISA	Interchange Control Header	M	1
GS	Functional Group Header	M	GS 1 > 1
GE	Functional Group Trailer	M	GE 1 > 1
IEA	Interchange Control Trailer	M	1

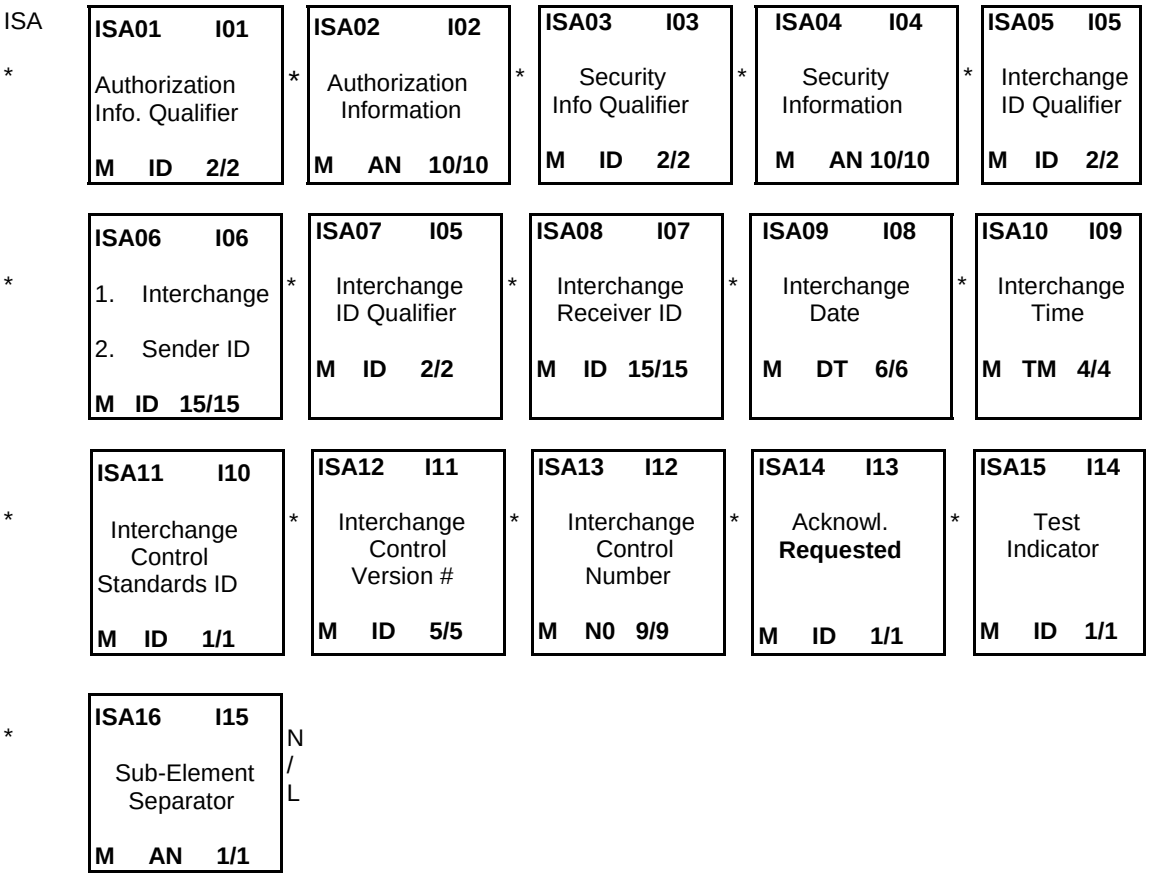
(M = mandatory)

Note: Segments GS01 and GS08 have been significantly changed in this release 3.02.

ISA

Interchange Control Header

Indicates the beginning of an interchange



ISA01 Authorization Information Qualifier
Code identifying the type of information in ISA02. Use “00” to indicate no authorization information is present.

ISA02 Authorization Information
Used for additional identification or authorization of the sender or data contained in the interchange. Not used

ISA03 Security Information Qualifier

Code identifying the type of information in ISA04. Use “00” to indicate no security information is present.

ISA04 Security Information
Identifies security information about the sender or data in the interchange.
Not used.

ISA05 Interchange ID Qualifier
Designates the code structure used to identify the sender. Defined by the sender.
For example, use “12” for Phone Number or “01” for DUNS.

ISA06 Interchange Sender ID
Published identification of the sender. Defined by the sender.

ISA07 Interchange ID Qualifier
Designates the code structure used to identify the receiver.
For example, use “12” for Phone Number or “01” for DUNS.

ISA08 Interchange Receiver ID
To be provided by the Receiver General (RG) in accordance with the Receiver General Test Plan and Release Procedures.

ISA09 Interchange Date
Date the interchange was created. Format must be “**YYMMDD**".

ISA10 Interchange Time
Time the interchange was created. Format must be “**HHMM**".

ISA11 Interchange Control Standards ID
Code designating the standards body. Use “**U**".

ISA12 Interchange Control Version Number
Version number of the interchange control segments. Use “**00200**".

ISA13 Interchange Control Number
Unique identifier for the interchange. Created by the sender and must be the same as IEA02.

ISA14 Acknowledgement Requested
Code indicating whether or not an acknowledgement is requested by the sender.
Receiver General will disregard.

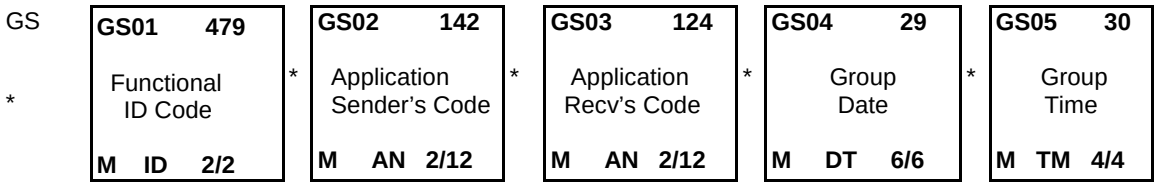
ISA15 Test Indicator
Code indicating whether the interchange contains test or production data.
Use either **“P” for production or “T” for test**.

ISA16 Sub-element Separator
Separating character for data element subgroups.
Receiver General will disregard.

GS

Functional Group Header

Indicates the beginning of a functional group of documents



*	**GS06 28** Group Control Number **M N0 1/9**	*	**GS07 455** Responsible Agency Code **M ID 1/2**	*	**GS08 480** Version/Release IND. ID Cd. **M ID 1/12**	N / L

GS01 Functional ID Code
Code identifying a group of application related transaction sets. Transaction sets and codes acceptable to the RG include:

Transaction Set	Code
821	FR
152	GR
820	RA
823	LB

GS02 Application Sender's Code
Code identifying the sender of the functional group.

GS03 Application Receiver's Code
Code identifying the receiver of the functional group. Use "**RECGEN**".

GS04 Group Date
Date the group was created. Format must be "**YYMMDD**".

GS05 Group Time
Time the group was created. Format must be "**HHMM**".

GS06 Group Control Number
Unique identifier of the group. Created by the sender and must be the same value as GE02.

GS07 Responsible Agency Code
Code identifying the standards agency used for this group. Value should be "**X**".

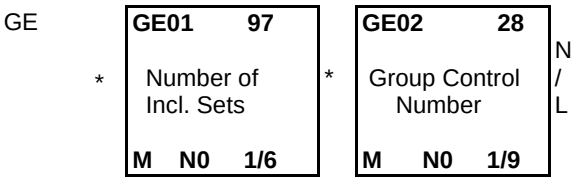
GS08 Version /Release /Industry Identifier Code
Receiver General's standard versions. Later versions may be supported if mutually agreed with the industry.

Transaction Set	Version
821, 820	"003010"
152, 823, 820	"003030"

GE

Functional Group Trailer

Indicates the end of a functional group of documents



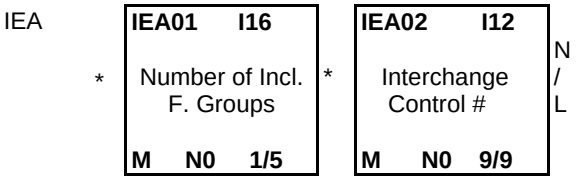
GE01 Number of Transaction Sets
Value must equal the number of transaction sets included in this functional group.

GE02 Group Control Number
Must be the same value as GS06.

IEA

Interchange Control Trailer

Indicates the end of an interchange



IEA01 Number of Included Functional Groups
Value must equal the number of functional groups contained in the interchange.

IEA02 Interchange Control Number
Unique identifier for the interchange. Must be the same as ISA13.

ANNEX A, APPENDIX 4

821 Mapping

821 MAPPING

VERSION 003010

(Receiver General Financial Information Reporting)

Release 2.12

821 Financial Information Reporting (X.12 version 3010)
Receiver General for Canada *(release 2.12)*

Upon mutual agreement with the industry, the Receiver General (RG) will support and supply mapping documents for versions above 3010.

Table 1

SEG. ID	Name	ANSI Req.	Max	R.G. Req	Min	Max	Loop
ST	Transaction set header	M	1	M	1	1	
BGN	Beginning segment	M	1	M	1	1	
N1	Name (forwarder of info)	M	1	M	1	1	**N1/1**
PER	Admin Comm. Contact	O	>1	O		>1	
N1	Name (Receiver of info)	M	1	M	1	1	**N1/>1**
PER	Admin Comm. Contact	O	>1	O		>1	
ACT	Account Identification	O	1	M	1	1	**ACT/1**
CUR	Currency	O	1	O		1	
BAL	Balance details	O	>1	M	1	>1	
FIR	Financial information	O	1	O	1	1	**FIR/>1**
REF	Reference numbers	O	>1	C	0	2	
SE	Transaction set trailer	M	1	M	1	1	

(M = mandatory; O = optional; C = conditional)

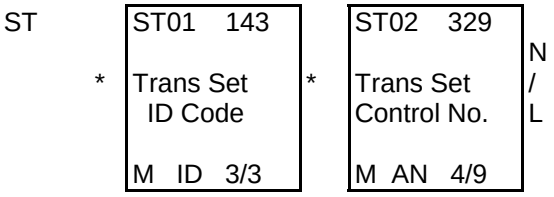
Notes:

1. N1 (preferred first occurrence) is the forwarder of the 821
2. N1 (preferred second occurrence) is the receiver of the 821 (the Receiver General)

Segments and data elements

ST
Transaction set header

Indicates the beginning of the transaction set

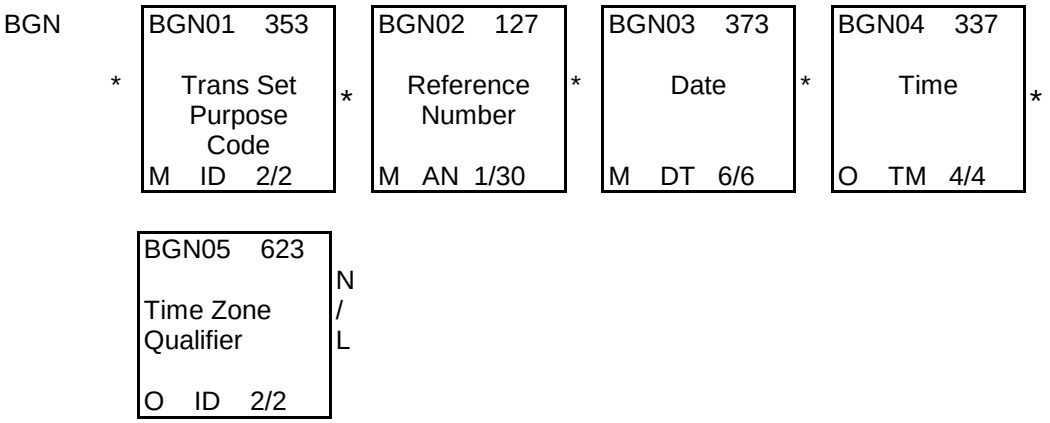


ST01 - Transaction set identifier code
Mandatory element with the value of "821"

ST02 - Transaction set control number
This control number is used to uniquely identify each document sent between trading partners. It is suggested that this number be incremented by one greater than the previous transaction.

BGN
Beginning segment

To indicate the beginning of a transaction set.



BGN01 - Code identifying purpose of transaction set.
Mandatory element with the value of "00" indicating income tax withholdings, installments or arrears or "22" indicating all other financial reporting.
Mandatory element for EDI standard but not used by RG.

BGN02 - Uniquely identifies the transaction set.
This number will be comprised of two components:
1. Four digit CPA Financial Institution (FI) ID indicating the originating FI
2. A combination of up to 26 digits, letters and or spaces that uniquely identifies the transaction.

BGN03 - Identifies the Banking Day when the account balance was noted.
(YYMMDD).

BGN04 - BGN05
Not used.

N1
NAME (preferred the 1st occurrence)

The first occurrence of the N1 segment identifies the Forwarder of the financial information.

N1		N101 98		N102 93		N103 66		N104 67	
	*	Entity ID Code.	*	Name	*	ID Code. Qualifier	*	ID Code	N / L
		M ID 2/2		M AN 1/35		C ID 1/2		C ID 2/17	

N101 - Entity ID code
Mandatory element with the value "FW" indicating the Forwarder.

N102 - Name
Name of the FI that is forwarding the information.

N103 - N104
Not used.

N1
NAME (preferred the 2nd occurrence)

The second occurrence of the N1 segment identifies the Receiver of the financial information.

N1		N101 98		N102 93		N103 66		N104 67	
	*	Entity ID Code.	*	Name	*	ID Code. Qualifier	*	ID Code	N / L
		M ID 2/2		M AN 1/35		C ID 1/2		C ID 2/17	

N101 - Entity ID code
Mandatory element with the value "AQ" indicating the "account of (destination party)".

N102 - Name

"REC GEN" "Receiver General for Canada"	Deposit Facilities transactions, CRA electronic remittances.
"205 REC GEN"	For all other remittances such as Bill Payment System (BPS).

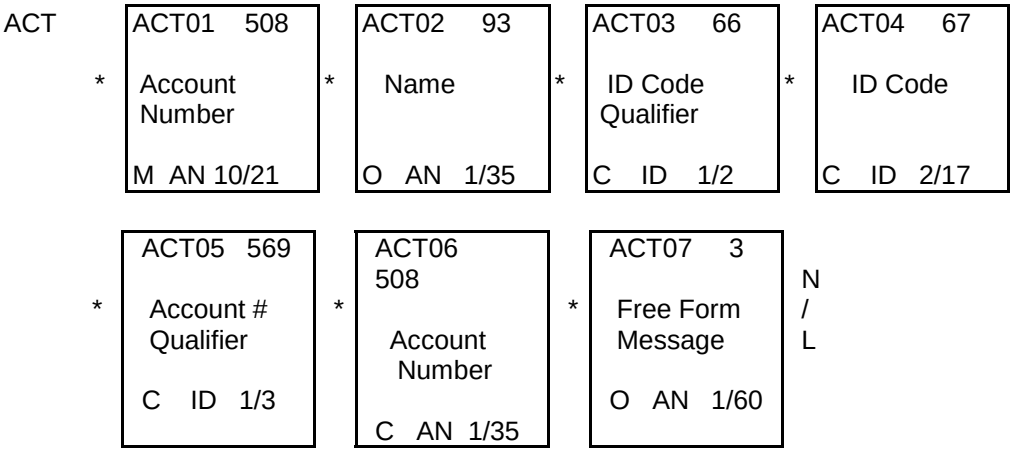
N103 - N104
Not used.

PER
Administrative Communications Contact

To identify a person or office to whom administrative communications should be directed. RG will disregard any data sent within this segment.

ACT
Account identification

To specify account information.



ACT01 - Account number
Identifies the FI, transit and account number for which the balance *is reported*.
The field is broken down as follows:

- CPA FI ID number char 1 - 4
- CPA Transit Number char 5 - 9
- Account Number char 10 - 21

Note: FI, transit and account number must be zero padded and right justified.

e.g.:

CPA FI ID number	0001
CPA Transit Number	9999
RG's Account Number	1234

ACT01 = **0001**0**9999**00000000**1234**

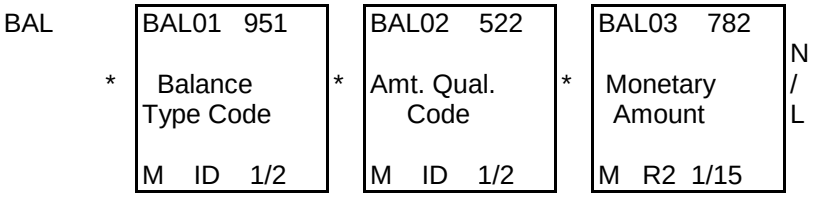
ACT02 - ACT07
Not used.

CUR
Currency

To specify the currency used in a transaction. RG will disregard any data sent within this segment.

BAL
Balance details

To identify the specific monetary balances associated with a particular account.



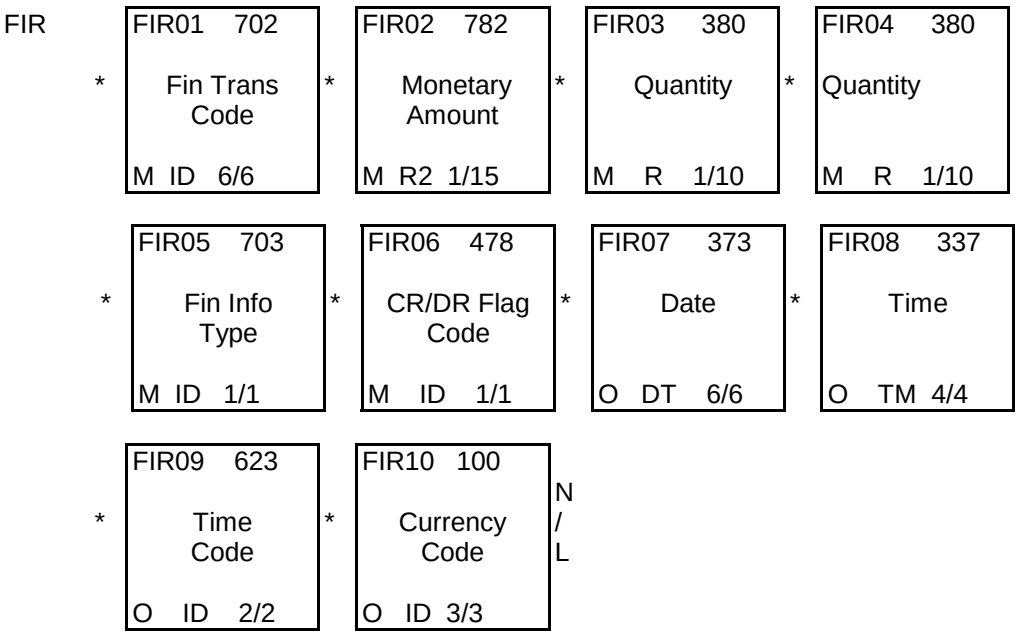
BAL01 - Balance type code
"Y" for "Year-to-date" to identify up-to-date/ current balance.

BAL02 - Qualifies the amount listed in BAL03
"IB" for "Investable Balance" (ie. available balance) or "NL" Negative Ledger Balance.

BAL03 - Qualified by the code in BAL02
Monetary balance of the account.

FIR
Financial information

To summarize a number of credit or debit transactions for a given account.



FIR01 - Identifies the type of transaction as described in Appendix 2, Section2. Separate codes must be provided for:

- Transactions Associated with Transfers to the Bank of Canada or between the sub-accounts and the concentrator account
- Wire Transfers
- Bank Initiated Adjustments Associated with Wire Transfers

- Direct Deposits
- Bank Initiated Adjustments Associated with Direct *Deposits*

FIR02 - Amount of the transaction
Must always be positive; FIR06 will flag credit or debit.

FIR03 - Quantity
Number of transactions included in the FIR02 account posting amount (deposit, etc.).

FIR04 Recommend use "1".

FIR05 - Identifies whether it is a detail or summary level of financial information.
Must equal “1” indicating “detail”.

FIR06 - Identifies whether FIR02 was a credit or debit to the account.
"C" for Credit, D for Debit.

FIR07 - Value date of transaction (YYMMDD).

FIR08 -FIR09
Not used.

FIR10 - Currency code
Code for country in whose currency the charges are specified.

REF
Reference numbers

REF		REF01 128 Reference # Qualifier M ID 2/2	*	REF02 127 Reference Number M AN 1/30	*	REF03 352 Description C AN 1/80	N/L

The RG reconciles deposit information based on the contents of the REF segment and it is conditional on the type of data being transmitted. The only instance in which an REF segment is not required is for Transfers to the Bank of Canada. The following is a table of the requirements of each data type.

Type of Financial Information Reporting (821)	**M or O**	**REF01 1st Occurrence**	**REF02 1st Occurrence**	**M or O**	**REF01 2nd Occurrence**	**REF02 2nd Occurrence**
H6 compliant 820’s or 823s where BGN = “22” (deposits, bank initiated adjustments reversing a deposit)	M	RR or ZZ	Unique cross reference tracer number also on the 820/823. May be variable in length.	M	PQ	8 digit CPA assigned “CCIN”
(returned items where permited, bank initiated adjustments reversing a returned item)	**O**	IX	Unique tracer that may be variable in length (e.g. Customer client number)	M	PQ	8 digit CPA assigned “CCIN”
820’s or 823s, other than above, where BGN01 = “00” / “22”	M	RR or ZZ		*M*	IT	

(deposits, bank initiated adjustments reversing a deposit) (returned items where permitted, bank initiated adjustments reversing a returned item)	 O	 IX	Unique cross reference tracer number also on the 820/823. May be variable in length. Unique tracer that may be variable in length (e.g. Customer client number)	 M	 IT	8 digit RG authorization number 8 digit RG authorization number
Electronic Card Transactions where BGN01 = "22" (deposits, bank initiated adjustments reversing a deposit) (returned items, bank initiated adjustments reversing a returned item)	**M*** **M**	IX IX	Unique tracer that may be variable in length (e.g. batch closure number) Unique tracer that may be variable in length (e.g. Customer client number)	M M	VR VR	Merchant Number **associated with transaction card type** (may be variable in length) Merchant Number **associated with transaction card type** (may be variable in length)
Deposit Facilities where BGN01 = "22" (deposits, bank initiated adjustments reversing a deposit) (returned items, bank initiated adjustments reversing a returned item)	 M M	 PB PB	 5 digit Transit Number from Originating Branch 5 digit Transit Number from Originating Branch	 M M	 IT IT	 8 digit RG authorization number 8 digit RG authorization number
Transfer to the BOC	O					
Wire transfer / *LVTS* (deposits, bank initiated adjustments)	O	IX	Unique tracer that may be variable in length (e.g. SWIFT #)	M	IT	8 digit RG authorization number
Direct Deposits (deposits, bank initiated adjustments)	O	IX	Unique tracer that may be variable in length (e.g. Direct Deposit file #)	M	IT	8 digit RG authorization number

Authorization, Merchant, Transit and Corporate Creditor Identification Numbers

Adjustments associated with the following element values must include the Tracer Number of the original deposit entry.

IT Provides the RG with their 8 digit authorization number identifying the departmental office which must be notified of the transaction. This reference is supplied to the FI by the transaction originator. NOTE: adjustments and returned item must include the 8 digit RG authorization number of the original deposit entry.

PB Provides the RG with the transit number of the branch at which the transaction was originated. Must be 5 characters in length.

SE
Transaction set trailer

Indicates the end of the transaction set.

SE		SE01 96		SE02 329		
	*	Number of Incl. Seg.	*	Trans Set Control No.		N / L
		M NO 1/6		M AN 4/9		

SE01 - Number of included segments
The value must equal the number of segments in the transaction set.

SE02 - Transaction set control number
Sender defined but it must equal the transaction set control number on the ST.

ANNEX A, APPENDIX 5

BANK OF CANADA LVTS FORMATTING REQUIREMENTS

SWIFT field code	SWIFT field name	Bank of Canada Required Information
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/550: 550:revenueaccount:date:amount; *repeatable* or /BNF/550: 550:revenueaccount:date:amount; *repeatable* or /REC/550: 550:revenueaccount:date:amount; *repeatable*

ANNEX A, APPENDIX 6

HISTORICAL AND FORECASTED EFT ACTIVITY

See spreadsheet attached

ANNEX A, APPENDIX 7

BANKING VALUES AND VOLUMES REMITTANCES FORECAST FOR 2014 TO 2018

See spreadsheet attached

ANNEX A, APPENDIX 7.1

FORECASTED OVER $50 M TRANSACTIONS: DIRECT DEPOSITS, WIRE TRANSFERS

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

Please note that the forecasts have been estimated by the RG on a « best efforts » basis.

ANNEX A, APPENDIX 8

EFT REQUEST FORM

***SETUP TYPE (Check One)*:** **New Set-up** **Amendment** **Closure**

PART 1: DEPARTMENTAL OFFICE INFORMATION

Department Name:	**Department Number :**	**Region Code:**
Program Description:		
Requested Implementation Date:		

Departmental Office Site Information:

Departmental Office Name (Doing Business As): **(bilingual, max. 30 characters; appears as Beneficiary Name on the payment instructions for incoming wires/direct deposits)**		
Address:	**City & Province**	**Postal Code:**
Primary Contact		
Name:	**Tel #:**	**Fax #:**
Contact Position:		
Email:		
Alternate Contact		
Name:	**Tel #:**	**Fax #:**
Contact Position:		
Email:		

Transaction Information:

Anticipated Monthly Volume of Transactions:	**Anticipated Monthly Dollar Value of Transactions:**

PART 2: BANKING INFORMATION

To be completed by the Receiver General (RG) and the Financial Institution (FI) for NEW facilities. To be completed by the Department for AMENDMENTS AND CLOSURES.

RG Authorlzation Number:	**FI Assigned Sub Account Number**	**Effective Date:**

Financial Institution Information:

Current EFT Service Provider:	**Transit:**	
Address:	**City, Province:**	**Postal Code:**

PART 3: ONLINE REPORTING TOOL USER SETUP

User # 1	
Name :	**Preferred Language:** English French
Phone Number:	**Fax Number:**
E-Mail Address:	
User # 2	
Name :	**Preferred Language:** English French
Phone Number:	**Fax Number:**
E-Mail Address:	

Online Reporting Tool User Setup Instructions

[INSTRUCTIONS TO BE INSERTED UPON CONTRACT AWARD]

PART 4: AUTHORIZATION

RECEIVER GENERAL REPRESENTATIVE	
Name:	
Title:	
Email :	
Phone :	**Fax :**
Signature:	**Date :**

FINANCIAL INSTITUTION OFFICER
Name:
Title:
Date:
Signature:
Effective Date :

Description of Fields

Field Name	Explanation
Setup Type	
Type: New, Amendment, Closure	**Check the appropriate option:** • *New Set-up*: creation of an EFT facility for the first time. • *Amendment*: changing the configuration of an existing EFT facility. • *Closure*: if an existing EFT facility needs to be closed.
PART 1: DEPARTMENTAL OFFICE INFORMATION	
Department Name, Number and Region Code	Input the official Department's name, its three-digit number and its three-digit region code if applicable.
Program Description	If this service is to be used for a specific program, please briefly describe. Otherwise leave this section blank.
Requested Implementation Date	Input the requested implementation date of the service. Please note that the setup process can take between two to six weeks to complete. The Department is therefore responsible for ensuring that the Setup Form is submitted six weeks in advance of the requested implementation date. The RG cannot guarantee the ability to meet the requested implementation if the Request Form is not submitted six weeks in advance.
Departmental office site information	
Departmental Office Name (DBA)	This is the name to appear as the Beneficiary Name on the payment instructions for incoming wires/direct deposits. It should be bilingual and up to a maximum of 30 characters. It is also known as Doing Business As (DBA).
Address and the two contact persons' details	Address of the location and the two contact persons' information for on-going support.
Transaction Information:	Please complete all fields.
PART 2: BANKING INFORMATION	
RG Authorization Number	For new requests, the RG will input the authorization number. For other requests, input the authorization # previously provided by the RG.
FI Assigned Sub Account Number	The FI will input the related Sub Account Number for new setups. The department is responsible to populate this field for amendments or closures.
Effective Date	Date the request is to take effect. To be completed by the RG Representative.
Financial Institution Information	Includes the name, address of the financial institution, and transit number.
PART 3: ONLINE REPORTING TOOL USER SETUP	
Name, phone number, fax number, email address	Input the information required about the User(s).
Preferred Language	The Online Reporting solution will be displayed to the User(s) in the language selected.
PART 4: AUTHORIZATION	
Receiver General Representative	The Receiver General representative will validate the information.

ANNEX B

BASIS OF PAYMENT

Contract Period: **The period of the contract is for three years from date of contract.**
During the period of the Contract, for Work performed in accordance with the Contract, the Contractor will be paid as specified below.

1.0 Transaction Fees:

Firm all inclusive transaction fees per EFT remittance

FIRM ALL-INCLUSIVE TRANSACTION FEES FOR DIRECT DEPOSIT AND WIRE TRANSFER					
Category	**Year 1**	**Year 2**	**Year 3**	**Option Year 1**	**Option Year 2**
Direct Deposit					
Firm all-inclusive Transaction Fee	$	$	$	$	$
Wire Transfer					
Firm all-inclusive Transaction Fee	$	$	$	$	$

If a transition period is required, the fees for the transition period will be the same as the fees applicable at the time of the transaction period notice issuance.

2.0 One-Time Departmental Office Setup Fees:

Charges to establish and maintain an additional departmental office with the capability of receiving EFT remittances. These fees include all administrative activities required to allow for this capability.

	Year 1	**Year 2**	**Year 3**	**Option Year 1**	**Option Year 2**
One-time Firm all-inclusive Departmental office Setup Fee	**$**	**$**	**$**	**$**	**$**

If a transition period is required, the fees for the transition period will be the same as the fees applicable at the time of the transaction period notice issuance.

3.0 Monthly Departmental Online User Access Fee:

Charges to establish and maintain online account access capability to each designated departmental office employee. These fees include all administrative activities required to provide this online access capability.

	Year 1	Year 2	Year 3	Option Year 1	Option Year 2
Monthly Firm all-inclusive Departmental online user access Fee (per user)	**$**	**$**	**$**	**$**	**$**

If a transition period is required, the fees for the transition period will be the same as the fees applicable at the time of the transaction period notice issuance.

4.0 Collateral Charges on Individual Transactions Greater Than, or Equal to, $50 million

A firm basis point spread (bps) rate will be paid on all individual transactions received that are greater than, or equal to, $50 million (≥ $50 M). As the Contractor must transfer funds to the RG's account at the BoC on the same day the funds were received for all transfers received before 14:00 EDT, and next day for any funds received after 14:00 EDT, we do understand that additional collateral may need to be raised on days when large value transactions are received. For this reason, we are providing a method for the Contractor to charge for collateral costs on individual transactions received that are greater than, or equal to, $50 million.

	Year 1	Year 2	Year 3	Option Year 1	Option Year 2
Firm all-inclusive Basis Point Spread (BPS) on transactions greater than, or equal to, $50 million					

If a transition period is required, the fees for the transition period will be the same as the fees applicable at the time of the transaction period notice issuance.

5.0 Total Estimated Cost - Contract Period: $ _____. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax (GST/HST) is extra, if applicable.

6.0 Total Estimated Cost - Extended Contract Period (From_____ to _____): $ _____. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax (GST/HST) is extra, if applicable.

ANNEX C

SECURITY REQUIREMENTS CHECK LIST

See attached

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).

ANNEX A, APPENDIX 6.1

HISTORICAL VALUES AND VOLUMES: DIRECT DEPOSITS (DD), WIRE TRANSFERS (WT)

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

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

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

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

Over $50M Transaction Details		
Date (DD/MM/YYYY)	Transaction Type	Transaction Amount
27/10/2011	WT	$ 50,000,000.00
27/10/2011	WT	$ 50,000,000.00
30/06/2011	WT	$ 50,082,778.00
30/03/2012	WT	$ 50,295,241.42
22/11/2011	WT	$ 50,464,348.00
30/03/2012	DD	$ 51,165,618.88
18/11/2011	DD	$ 51,620,713.01
01/12/2011	WT	$ 55,104,292.50
30/06/2011	WT	$ 55,487,429.32
29/06/2011	WT	$ 57,000,000.00
30/03/2012	WT	$ 58,821,932.61
21/03/2012	WT	$ 63,508,341.17
19/07/2011	WT	$ 65,427,973.00
14/02/2012	WT	$ 68,961,892.90
01/06/2011	WT	$ 70,496,491.06
01/06/2011	WT	$ 79,794,407.53
01/09/2011	WT	$ 79,952,143.78
01/09/2011	DD	$ 79,952,143.78
31/08/2011	WT	$ 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	WT	$ 82,978,510.89
04/11/2011	WT	$ 83,000,000.00
28/02/2012	DD	$ 84,100,000.00
15/03/2012	WT	$ 85,180,677.00
19/03/2012	WT	$ 87,166,148.92
30/03/2012	WT	$ 91,159,217.77
30/03/2012	DD	$ 93,418,277.10
01/06/2011	WT	$ 93,888,718.45
11/04/2011	WT	$ 99,477,500.00
01/06/2011	WT	$ 106,441,246.15
11/04/2011	WT	$ 109,855,608.22
01/09/2011	WT	$ 116,094,789.05
01/09/2011	DD	$ 116,094,789.05
01/09/2011	WT	$ 116,287,059.45

Over $50M Transaction Details		
Date (DD/MM/YYYY)	Transaction Type	Transaction Amount
29/11/2012	DD	$ 51,353,032.07
24/05/2012	WT	$ 52,842,600.00
20/06/2012	WT	$ 52,925,000.00
12/10/2012	WT	$ 54,906,597.00
11/12/2012	WT	$ 55,000,000.00
01/06/2012	WT	$ 60,087,162.86
12/07/2012	WT	$ 60,352,717.02
01/06/2012	WT	$ 61,133,515.16
01/06/2012	WT	$ 62,414,819.08
20/11/2012	WT	$ 64,233,841.52
27/12/2012	WT	$ 64,242,432.09
29/06/2012	WT	$ 68,623,566.00
31/05/2012	WT	$ 70,344,393.70
01/06/2012	WT	$ 72,096,108.79
20/04/2012	WT	$ 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	WT	$ 89,833,379.38
01/06/2012	WT	$ 95,216,451.42
01/06/2012	WT	$ 96,256,650.66
01/06/2012	WT	$ 96,462,352.99
31/05/2012	WT	$ 97,220,970.80
01/06/2012	WT	$ 101,893,855.26
01/10/2012	WT	$ 115,662,102.55
02/04/2012	WT	$ 119,430,202.84
01/06/2012	WT	$ 122,032,155.92
01/06/2012	WT	$ 122,276,062.44
01/06/2012	WT	$ 123,256,983.14
31/12/2012	WT	$ 141,824,423.21
03/07/2012	WT	$ 143,033,276.31
18/06/2012	WT	$ 210,343,327.93
01/06/2012	WT	$ 213,459,306.83
15/06/2012	WT	$ 226,357,165.38
01/06/2012	WT	$ 232,344,615.29
01/06/2012	WT	$ 239,854,399.85

31/03/2011	WT	$ 496,000,000.00
20/04/2010	WT	$ 733,405,891.07

01/06/2011	WT	$ 118,086,223.89
18/04/2011	WT	$ 122,057,718.29
01/09/2011	WT	$ 122,252,672.72
01/09/2011	DD	$ 122,252,672.72
30/09/2011	WT	$ 122,574,369.48
01/09/2011	WT	$ 123,030,798.92
01/09/2011	DD	$ 123,030,798.92
01/06/2011	WT	$ 124,777,442.89
01/06/2011	WT	$ 135,251,130.57
16/06/2011	WT	$ 135,268,968.98
01/06/2011	WT	$ 147,180,702.01
30/06/2011	WT	$ 149,388,324.02
21/11/2011	WT	$ 160,402,213.46
01/06/2011	WT	$ 179,079,575.96
01/06/2011	WT	$ 211,311,537.92
03/01/2012	WT	$ 212,684,770.44
30/03/2012	WT	$ 319,800,000.00
01/06/2011	WT	$ 328,123,931.76
21/12/2011	WT	$ 340,100,000.00
01/04/2011	WT	$ 346,799,000.00
30/03/2012	WT	$ 362,792,452.00
01/06/2011	WT	$ 493,981,043.77
15/03/2012	WT	$ 500,000,000.00
24/05/2011	WT	$ 500,000,000.00
24/05/2011	WT	$ 634,018,507.58
30/03/2012	WT	$ 660,528,781.41

01/06/2012	WT	$ 240,789,043.37
13/04/2012	WT	$ 248,237,091.39
09/04/2012	WT	$ 249,156,669.20
09/04/2012	WT	$ 250,872,931.64
01/06/2012	WT	$ 281,910,909.22
07/05/2012	WT	$ 300,947,533.86
01/06/2012	WT	$ 324,785,990.63
02/04/2012	WT	$ 371,616,000.00
01/06/2012	WT	$ 397,600,292.50
01/06/2012	WT	$ 438,273,453.86
09/01/2013	WT	54,560,000
10/01/2013	WT	74,356,667.63
21/01/2013	WT	120,409,013.18

ANNEX A, APPENDIX 6.2

WEEKLY INCOMING WIRE TRANSFER VOLUMES

Legend:

	Week extended in next month

Timeframe	April 2010 to March 2011			April 2011 to March 2012			April 2012 to March 2013		
Month	Week	Wire Count	Total $ Amount	Week	Wire Count	Total $ Amount	Week	Wire Count	Total $ Amount
April	5 AP	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 AP	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
May	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
June	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
July	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 AU	233	$ 46,162,175
	Total	245	$ 237,228,642	Total	1,053	$ 477,849,995	Total	2,049	$ 934,052,630
August	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 AU	21	$ 36,113,198	5 AU	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
September	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

MONTHLY INCOMING WIRE TRANSFER VOLUMES

Timeframe	2010/2011		2011/2012		2012/2013	
Month	Wire Count	Total $ Amount	Wire Count	Total $ Amount	Wire Count	Total $ Amount
April	125	$ 1,402,413,015	808	$ 1,124,424,514	1,755	$ 1,883,877,102
May	199	$ 106,101,254	877	$ 1,513,007,297	1,400	$ 1,067,757,760
June	283	$ 695,562,580	970	$ 3,008,600,065	1,348	$ 4,425,295,475
July	265	$ 246,754,784	1,053	$ 477,849,995	1,816	$ 887,890,455
August	219	$ 454,622,766	989	$ 486,727,912	1,424	$ 425,104,730
September	226	$ 433,530,205	994	$ 1,079,596,034	1,229	$ 287,816,305
October	250	$ 1,134,098,784	1,147	$ 439,764,091	1,865	$ 628,039,259
November	230	$ 263,002,072	1,122	$ 742,227,953	1,513	$ 476,255,896
December	324	$ 775,539,164	1,155	$ 1,104,659,662	1,504	$ 932,317,659
January	313	$ 374,200,449	1,357	$ 679,593,455	2,307	$ 782,118,921
February	558	$ 324,490,969	1,662	$ 637,424,925		
March	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

	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
October	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
	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
November	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
December	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
January	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
February	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		
March	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 ADJUSTED*	10/11	3,703	$ 8,927,087,147	11/12	13,783	$ 14,417,136,518	12/13		

* Adjustment for the transactions of next fiscal year included in the count for current fiscal year

ANNEX A, APPENDIX 6.3

INCOMING DIRECT DEPOSIT VOLUMES

Legend:

	Week includes first days of next month

Timeframe	April 2010 to March 2011			April 2011 to March 2012			April 2012 to March 2013		
Month	Week	DD Count	Total $ Amount	Week	DD Count	Total $ Amount	Week	DD Count	Total $ Amount
April	5 AP	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 AP	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
May	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
June	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
July	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 AU	75	$ 13,320,516
	Total	82	$ 9,657,215	Total	476	$ 99,722,809	Total	541	$ 176,410,213
August	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
	5A	35	$ 8,874,345	5A	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
September	1	19	$ 998,442	1	69	$ 52,259,350	1	84	$ 8,263,693

Timeframe	2010/2011		2011/2012		2012/2013	
Month	DD Count	Total $ Amount	DD Count	Total $ Amount	DD Count	Total $ Amount
April	51	$ 2,175,836	342	$ 48,191,134	471	$ 134,760,624
May	65	$ 10,057,859	374	$ 109,062,293	505	$ 94,316,963
June	83	$ 10,845,464	430	$ 179,557,195	520	$ 344,702,384
July	90	$ 13,432,527	476	$ 99,722,809	466	$ 163,089,697
August	139	$ 25,456,761	528	$ 91,937,380	501	$ 138,105,208
September	143	$ 9,595,203	349	$ 672,076,689	436	$ 120,863,040
October	172	$ 25,622,539	367	$ 113,781,723	587	$ 305,528,092
November	179	$ 39,881,784	429	$ 157,452,115	583	$ 280,541,728
December	180	$ 37,392,423	390	$ 263,124,295	451	$ 301,563,882
January	210	$ 21,549,702	431	$ 167,257,204	596	$ 109,974,236.12
February	257	$ 97,973,031	422	$ 213,878,396		
March	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

	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
October	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
	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
November	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
December	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
January	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
February	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			
March	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 ADJUSTED*	10/11	1,895	$ 504,069,800	11/12	5,016	$ 2,448,958,759	12/13		

* Adjustment for the transactions of next fiscal year included in the count for current fiscal year

ANNEX A, APPENDIX 7

FORECASTED ESTIMATED ANNUAL VALUES AND VOLUMES: DIRECT DEPOSITS, WIRE TRANSFERS

	Fiscal Year 2013-2014				Fiscal Year 2014-2015				Fiscal Year 2015-2016				Fiscal Year 2016-2017				Fiscal Year 2017-2018			
	DD Count	DD Value	WT Count	WT Value	DD Count	DD Value	WT Count	WT Value	DD Count	DD Value	WT Count	WT Value	DD Count	DD Value	WT Count	WT Value	DD Count	DD Value	WT Count	WT Value
April	495	$141,498,655	1,843	$1,978,070,957	519	$148,573,588	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
May	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
June	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
July	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
August	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
September	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
October	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
November	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
December	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
January	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
February	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
March	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

Please note that the forecasts have been estimated by the RG on a « best efforts » basis.

Based on 2011-2012 (5% for yr 2012/13, 2013/14)
Based on 2012-2013 (5% for yr 2013/14)

Attachment 1 to Annex C – Information Technology Security Requirements (ITSR)

The Contractor must demonstrate that any Information Technology (IT) system(s) and/or application(s) that will be used in the delivery of the EFT service meet the Baseline Requirements identified herein. If applicable to the proposed EFT solution(s) and as determined by the project authority, the Contractor must also demonstrate that any IT system(s) and/or application(s) that will be used in the delivery of the EFT service meet the Supplemental Requirements.

Demonstration of compliance with the Baseline and applicable Supplemental requirements identified below will be done at Canada's request after contract award.

1.1 Policy & Procedures (PP)

The following table lists the ITSR related to the Policy and Procedure across all domains of IT Security for the EFT Service.

Table C-1: PP Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PP-01	POLICY AND PROCEDURES	• The service provider develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among service provider entities, and compliance for the following at a minimum annually. ○ Access Control ○ Security Awareness and Training ○ Audit and Accountability ○ Security Assessment and Authorization ○ Configuration Management ○ Contigency Planning ○ Identification & Authentication ○ Incident Response ○ System Maintenance ○ Media Protection ○ Physical & Environmental ○ Security Planning ○ Personnel Security ○ Risk Assessment ○ System & Services Acquisition	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ Security Function Isolation ○ System & Information Integrity • The service provider develops, disseminates, and reviews/updates a formal, documented procedures to facilitate the implementation of the policies and associated controls for the following at a minimum annually: ○ access control. ○ security awareness and training. ○ audit and accountability. ○ security assessment and authorization. ○ configuration management policy and associated configuration management controls. ○ contingency planning, including an audit cycle for the contingency plan program as the basis of regular reporting to TBS. ○ identification and authentication. ○ incident response including the incorporation of heightened levels of readiness during emergency and heightened IT threat situations in accordance with the TBS Operational Security Standard - Readiness Levels for Federal Government Facilities and the TBS Operational Security Standard - Management of Information Technology Security. ○ information system maintenance. ○ media protection. ○ physical and environmental. ○ security planning. ○ personnel security. ○ risk assessment. ○ system and services acquisition. ○ system and communications protection. ○ system and information integrity.	✓	

1.2 Access Control (AC)

The following table lists the ITSR related to the AC domain for the EFT Service.

Table C-2: AC Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
AC-02	ACCOUNT MANAGEMENT	• The service provider manages information system accounts, including ○ identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). ○ establishing conditions for group membership. ○ identifying authorized users of the information system and specifying access privileges. ○ requiring appropriate approvals for requests to establish accounts. ○ establishing, activating, modifying, disabling, and removing accounts. ○ specifically authorizing and monitoring the use of guest/anonymous and temporary accounts. ○ notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. ○ Deactivating temporary accounts that are no longer required; and accounts of terminated or transferred users. ○ granting access to the system based on a valid access authorization; intended system usage; and other attributes as required by The service provider or associated missions/business functions. ○ review of accounts at a minimum annually.	✓	
AC-02-01	ACCOUNT MANAGEMENT	• The service provider ○ employs automated mechanisms to support the management of information system accounts. ○ Requires that system automatically logs out the users when 15 minutes of inactivity;		✓

ID	Requirement Title	Description	Baseline	Supplemental
		○ Determines normal time-of-day and duration usage for information system accounts; ○ Monitors for atypical usage of information system accounts; ○ Reports atypical usage to designated service provider officials; ○ Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and ○ Tracks and monitors privileged role assignments. • The information system automatically ○ terminates temporary and emergency accounts after a formally defined and documented time period for each type of account. ○ disables inactive accounts after a formally defined and documented time period. ○ audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.		✓
AC-03	ACCESS ENFORCEMENT	• The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	✓	
AC-03-01	ACCESS ENFORCEMENT	• The information system enforces a Discretionary Access Control (DAC) policy that: ○ Allows users to specify and control sharing by named individuals or groups of individuals, or by both; ○ Limits propagation of access rights; and ○ Includes or excludes access to the granularity of a single user.		✓
AC-04	INFORMATION FLOW ENFORCEMENT	• The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	✓	

ID	Requirement Title	Description	Baseline	Supplemental

AC-05	SEPARATION OF DUTIES	• The service provider
		  ○ separates duties of individuals as necessary, to prevent malevolent activity without collusion.
		  ○ documents separation of duties.
		  ○ implements separation of duties through assigned information system access authorizations.
			✓	

AC-06	LEAST PRIVILEGE	• The service provider employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with service provider missions and business functions.	✓	
AC-06-01	LEAST PRIVILEGE	• The service provider explicitly authorizes access to security functions deployed in hardware, software, and firmware and security-relevant information. • The service provider requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and audits any use of privileged accounts, or roles, for such functions. • The service provider limits authorization to super user accounts on the information system to designated system administration personnel.		✓ ✓ ✓

AC-07	UNSUCCESSFUL LOGIN ATTEMPTS	• The information system enforces a limit of THREE consecutive invalid login attempts by a user during a day.
		• The information system automatically:
		  ○ Locks the account/node for a system configurable time period.
		  ○ Locks the account/node until released by an administrator.
		  ○ Delays next login prompt according to a system configurable value when the maximum number of unsuccessful attempts is exceeded regardless of
			✓
			✓	

ID	Requirement Title	Description	Baseline	Supplemental
		whether the login occurs via a local or network connection.		
AC-08	SYSTEM USE NOTIFICATION	• The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks • The information system retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system. • The information system, for publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	✓ ✓ ✓	
AC-09	PREVIOUS LOGON (ACCESS) NOTIFICATION	• The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	✓	
AC-09-01	PREVIOUS LOGON (ACCESS) NOTIFICATION	• The information system notifies the user ○ upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access. ○ number of unsuccessful logon/access attempts during a system configurable time period. ○ security-related changes to the user's account during a system configurable time period.		✓
AC-11	SESSION LOCK	• The information system prevents further access to the system by initiating a session lock after a system configurable time period of inactivity or upon receiving a request from a user. • The information system retains the session lock until the user re-	✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
		establishes access using established identification and authentication procedures.		
AC-11-01	SESSION LOCK	• The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.		✓
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	• The service provider identifies specific user actions that can be performed on the information system without identification or authentication. • The service provider documents and provides supporting rationale in the operations security plan for the information system, user actions not requiring identification and authentication.	✓ ✓	
AC-14-01	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	• The service provider permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.		✓
AC-16	SECURITY ATTRIBUTES	• The information system supports and maintains the binding of security attributes to information in storage, in process, and in transmission.	✓	
AC-16-01	SECURITY ATTRIBUTES	• The information system allows authorized entities to change security attributes. • The information system allows authorized users to associate security attributes with information. • The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify special dissemination, handling, or distribution instructions using human readable, standard naming conventions.		✓ ✓ ✓
AC-17	REMOTE ACCESS	• The service provider ○ documents allowed methods of remote access to the information system.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ establishes usage restrictions and implementation guidance for each allowed remote access method. ○ monitors for unauthorized remote access to the information system. ○ authorizes remote access to the information system prior to connection. ○ enforces requirements for remote connections to the information system. ○ ensures that all employees working off site safeguard information as per the minimum requirements in accordance with the TBS Operational Security Standard on Physical Security.		
AC-17-01	REMOTE ACCESS	• The service provider ○ employs automated mechanisms to facilitate the monitoring and control of remote access methods. ○ uses cryptography to protect the confidentiality and integrity of remote access sessions. The cryptography must be compliant with the requirements of control SC-13. ○ authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. ○ monitors for unauthorized remote connections to the information system, and takes appropriate action if an unauthorized connection is discovered at a minimum annually. ○ ensures that users protect information about remote access mechanisms from unauthorized use and disclosure. ○ ensures that remote sessions for accessing security functions and security-relevant information employ additional security measures and are audited. ○ disables deemed non-secure networking protocols within the information system except for explicitly identified		✓

ID	Requirement Title	Description	Baseline	Supplemental
		components in support of specific operational requirements. • The information system routes all remote accesses through a limited number of managed access control points. • Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g. Internet access not allowed).		✓ ✓
AC-18	WIRELESS ACCESS	• The service provider ○ establishes usage restrictions and implementation guidance for wireless access. ○ monitors for unauthorized wireless access to the information system. ○ authorizes wireless access to the information system prior to connection. ○ enforces requirements for wireless connections to the information system.	✓	
AC-18-01	WIRELESS ACCESS	• The information system protects wireless access to the system using authentication and encryption. • The service provider at a minimum annually ○ monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, and takes appropriate action if an unauthorized connection is discovered. ○ does not allow users to independently configure wireless networking capabilities. ○ disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.		✓ ✓
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	• The service provider ○ establishes usage restrictions and implementation guidance for organization-controlled mobile devices.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ authorizes connection of mobile devices meeting service provider usage restrictions and implementation guidance to service provider information systems. ○ monitors for unauthorized connections of mobile devices to service provider information systems. ○ enforces requirements for the connection of mobile devices to service provider information systems. ○ disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction. ○ issues specially configured mobile devices to individuals traveling to locations that the service provider deems to be of significant risk in accordance with service provider policies and procedures. ○ applies inspection and preventative measures to mobile devices returning from locations that The service provider deems to be of significant risk in accordance with service provider policies and procedures.		
AC-19-01	ACCESS CONTROL FOR MOBILE DEVICES	• The service provider ○ restricts the use of writable, removable media in service provider information systems. ○ prohibits the use of personally owned, removable media in service provider information systems. ○ prohibits the use of removable media in service provider information systems when the media has no identifiable owner. ○ ensures that users turn off wireless devices with a voice transmission capability or physically disable the microphone when attending a meeting at which Protected B, Protected C or classified information is being shared as per the TBS Operational Security Standard - Management of Information Technology Security		✓ ✓ ✓ ✓
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	• The service provider establishes terms and conditions,	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to ○ access the information system from the external information systems. ○ process, store, and/or transmit organization-controlled information using the external information systems.		
AC-20-01	USE OF EXTERNAL INFORMATION SYSTEMS	• The service provider permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the service provider : (a) Can verify the implementation of required security controls on the external system as specified in the service provider 's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the service provider entity hosting the external information system. • The service provider limits the use of organization-controlled portable storage media by authorized individuals on external information systems.		✓ ✓
AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	• The service provider ○ facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances. ○ employs organization-defined information sharing circumstances and mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.	✓	
AC-21-01	USER-BASED COLLABORATION AND INFORMATION SHARING	• The service provider ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.		✓

ID	Requirement Title	Description	Baseline	Supplemental
AC-22	PUBLICLY ACCESSIBLE CONTENT	• The service provider ○ designates individuals authorized to post information onto an service provider information system that is publicly accessible. ○ trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information. ○ reviews the proposed content of publicly accessible information for confidentially sensitive information prior to posting onto the service provider al information system. ○ reviews the content on the publicly accessible service provider information systemfor confidentially sensitive information at a minimum annually. ○ removes confidentially sensitive information from the publicly accessible service provider information system, if discovered	✓	

1.3 Audit & Accountability (AU)

The following table lists the ITSR related to the AU domain for the EFT Service.

Table C-3: AU Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
AU-02	AUDITABLE EVENTS	• The service provider determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing all the auditable events. • The service provider coordinates the security audit function with other service provider entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. • The service provider provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents. • The service provider determines, based on current threat information and ongoing assessment of risk, that the events are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.	✓ ✓ ✓ ✓	
AU-02-01	AUDITABLE EVENTS	• The service provider reviews and updates the list of auditable events at a minimum annually. • The service provider includes execution of privileged functions in the list of events to be audited by the information system.		✓ ✓
AU-03	CONTENT OF AUDIT RECORDS	• The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	✓	
AU-03-01	CONTENT OF AUDIT	• The information system includes detailed audit event		✓

ID	Requirement Title	Description	Baseline	Supplemental
	RECORDS	information in the audit records for audit events identified by type, location, or subject.		
AU-04	AUDIT STORAGE CAPACITY	• The service provider allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	✓	
AU-05	RESPONSE TO AUDIT PROCESSING FAILURES	• The information system alerts designated service provider officials in the event of an audit processing failure. • The information system takes the additional actions e.g., shut down information system, overwrite oldest audit records, stop generating audit records.	✓ ✓	
AU-05-01	RESPONSE TO AUDIT PROCESSING FAILURES	• The information system provides a warning when allocated audit record storage volume reaches a system configurable percentage of maximum audit record storage capacity.		✓
AU-06	AUDIT REVIEW, ANALYSIS, AND REPORTING	• The service provider reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated service provider officials continously at regular periods. • The service provider adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to service provider operations, service provider assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information.	✓ ✓	
AU-06-01	AUDIT REVIEW, ANALYSIS, AND REPORTING	• The information system integrates audit review, analysis, and reporting processes to support service provider processes for investigation and response to suspicious activities. • The service provider analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. • The information system centralizes the review and analysis of audit records from multiple components within the system. • The service provider specifies the permitted actions for each		✓ ✓ ✓

ID	Requirement Title	Description	Baseline	Supplemental
		authorized information system process, role, and/or user in the audit and accountability policy.		✓
AU-07	AUDIT REDUCTION AND REPORT GENERATION	• The information system provides an audit reduction and report generation capability.	✓	
AU-07-01	AUDIT REDUCTION AND REPORT GENERATION	• The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		✓
AU-08	TIME STAMPS	• The information system uses internal system clocks to generate time stamps for audit records.	✓	
AU-08-01	TIME STAMPS	• The information system synchronizes internal information system clocks with an authoritative time source at a minimum annually.		✓
AU-09	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	✓	
AU-09-01	PROTECTION OF AUDIT INFORMATION	• The information system backs up audit records onto a different system or media than the system being audited on a regular basis. • The service provider : (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.		✓ ✓
AU-10	NON-REPUDIATION	• The information system protects against an individual falsely denying having performed a particular action.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
AU-10-01	NON-REPUDIATION	• The information system associates the identity of the information producer with the information. • The information system validates the binding of the information producer's identity to the information. • The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released. • The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain. • The service provider employs cryptography compliant with the requirements of control SC-13 to implement digital signatures.		✓ ✓ ✓ ✓ ✓
AU-11	AUDIT RECORD RETENTION	• The service provider retains audit records for a time period consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and service provider information retention requirements.	✓	
AU-12	AUDIT GENERATION	• The information system provides audit record generation capability for the auditable events defined in AU-2 at information system components. • The information system allows designated service provider personnel to select which auditable events are to be audited by specific components of the system. • The information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	✓ ✓ ✓	
AU-12-01	AUDIT GENERATION	• The information system compiles audit records from information system components into a system-wide (logical or physical) audit trail that is time-correlated to within a system configurable level of tolerance for relationship between time stamps of individual records in the audit trail.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.		✓

1.4 Certification Accreditation and Security Assessment (CA)

The following table lists the ITSR related to the CA domain for the EFT Service.

Table C-4: CA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CA-02	SECURITY ASSESSMENTS	• The service provider develops a security assessment plan that describes the scope of the assessment including: (a) Security controls and control Supplementals under assessment; (b) Assessment procedures to be used to determine security control effectiveness; and (c) Assessment environment, assessment team, and assessment roles and responsibilities.	✓	
		• The service provider assesses the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security control requirements for the system regularly.	✓	
		• The service provider produces a security assessment report that documents the results of the assessment.	✓	
		• The service provider provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	✓	
CA-02-01	SECURITY ASSESSMENTS	• The service provider includes at minimum the following as part of security control assessments at regular intervals, ○ announced ○ unannounced ○ in-depth monitoring ○ malicious user testing ○ penetration testing ○ red team exercises		✓

ID	Requirement Title	Description	Baseline	Supplemental
CA-03	INFORMATION SYSTEM CONNECTIONS	• The service provider authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements. • The service provider documents, for each connection, the interface characteristics, security control requirements, and the nature of the information communicated. • The service provider monitors the information system connections on an ongoing basis verifying enforcement of security control requirements.	✓ ✓ ✓	
CA-05	PLAN OF ACTION AND MILESTONES	• The service provider ○ develops a plan of action and milestones for the information system to document. ○ planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. ○ updates existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities at a minimum annually.	✓	
CA-06	SECURITY AUTHORIZATION	• The service provider ○ assigns a senior-level executive or manager to the role of authorizing official for the information system. ○ ensures that the authorizing official authorizes the information system for processing before commencing operations. ○ updates the security authorization at a minimum annually.	✓	
CA-07	CONTINUOUS MONITORING	• The service provider establishes a continuous monitoring strategy and implements a continuous monitoring program that includes	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ a configuration management process for the information system and its constituent components. ○ a determination of the security impact of changes to the information system and environment of operation. ○ ongoing security control assessments in accordance with the service provider's continuous monitoring strategy. ○ reporting the security state of the information system to appropriate service provider officials at a minimum annually.		
CA-07-01	CONTINUOUS MONITORING	• The service provider plans, schedules, and conducts assessments at a minimum annually, ○ announced ○ unannounced ○ in-depth monitoring ○ malicious user testing ○ penetration testing ○ red team exercises to ensure compliance with all vulnerability mitigation procedures.		✓

1.5 Configuration Management (CM)

The following table lists the ITSR related to the CM domain for the EFT Service.

Table C-5: CM Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CM-02	BASELINE CONFIGURATION	• The service provider develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	✓	
CM-02-01	BASELINE CONFIGURATION	• The service provider reviews and updates the baseline configuration of the information system: (a) At a minimum annually; (b) When required due to valid circumstances (documented and formally approved); and (c) As an integral part of information system component installations and upgrades. • The service provider employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. • The service provider : (a) Develops and maintains software programs authorized to execute on the information system; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. • The service provider maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.		✓ ✓ ✓ ✓
CM-03	CONFIGURATION CHANGE CONTROL	• The service provider ○ employs mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base. ○ determines the types of changes to the information system that are configuration controlled.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ approves configuration-controlled changes to the system with explicit consideration for security impact analyses. ○ documents approved configuration-controlled changes to the system. ○ retains and reviews records of configuration-controlled changes to the system. ○ audits activities associated with configuration-controlled changes to the system. ○ coordinates and provides oversight for configuration change control activities through configuration change control element that convenes at a minimum annually. ○ tests, validates, and documents changes to the information system before implementing the changes on the operational system. ○ requires an information security representative to be a member of the configuration change control element.		
CM-04	SECURITY IMPACT ANALYSIS	• The service provider analyzes changes to the information system to determine potential security impacts prior to change implementation.	✓	
CM-04-01	SECURITY IMPACT ANALYSIS	• The service provider analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. • The service provider , after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security control requirements for the system.		✓ ✓
CM-05	ACCESS RESTRICTIONS FOR CHANGE	• The service provider defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	✓	

ID	Requirement Title	Description	Baseline	Supplemental

CM-05-01	ACCESS RESTRICTIONS FOR CHANGE	• The service provider
		  ○ employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
		  ○ At a minimum annually conducts audits of information system changes and when indications so warrant determining whether unauthorized changes have occurred.
		  ○ Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and
		  ○ Reviews and re-evaluates information system developer/integrator privileges at a minimum annually.
		  ○ limits privileges to change software resident within software libraries (including privileged programs).
		• The information system automatically implements safeguards and countermeasures if security functions (or mechanisms) are changed inappropriately.
				✓
				
				✓

CM-06	CONFIGURATION SETTINGS	• The service provider
		  ○ establishes and documents mandatory configuration settings for information technology products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements.
		  ○ implements the configuration settings.
		  ○ identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.
		  ○ monitors and controls changes to the configuration settings in accordance with service provider policies and procedures.
			✓	

ID	Requirement Title	Description	Baseline	Supplemental

CM-06-01	CONFIGURATION SETTINGS	• The service provider
		  ○ employs automated mechanisms to centrally manage, apply, and verify configuration settings.
		  ○ employs automated mechanisms to respond to unauthorized changes to configuration settings.
		  ○ incorporates detection of unauthorized, security-relevant configuration changes into the service provider 's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.
		• The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.
				✓
				
				✓

CM-07	LEAST FUNCTIONALITY	• The service provider configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services prohibited or restricted functions, ports, protocols, and/or services.	✓	

CM-07-01	LEAST FUNCTIONALITY	• The service provider
		  ○ At a minimum annually reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.
		  ○ ensures compliance with registration requirements for ports, protocols, and services.
				✓

CM-08	INFORMATION SYSTEM COMPONENT INVENTORY	• The service provider develops, documents, and maintains an inventory of information system components that
		  ○ accurately reflects the current information system.
		  ○ is consistent with the authorization boundary of the information system.
		  ○ is at the level of granularity deemed necessary for
			✓	

ID	Requirement Title	Description	Baseline	Supplemental
		tracking and reporting. ○ includes information deemed necessary to achieve effective property accountability. ○ available for review and audit by designated service provider officials.		
CM-08-01	INFORMATION SYSTEM COMPONENT INVENTORY	• The service provider ○ updates the inventory of information system components as an integral part of component installations, removals, and information system updates. ○ employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. ○ employs automated mechanisms to detect the addition of unauthorized components/devices into the information system; ○ Disables network access by such components/devices or notifies designated service provider officials. ○ includes in property accountability information for information system components, a means for identifying by ○ name ○ position ○ role individuals responsible for administering those components. ○ verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. ○ includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.		✓

ID	Requirement Title	Description	Baseline	Supplemental
CM-09	CONFIGURATION MANAGEMENT PLAN	• The service provider develops, documents, and implements a configuration management plan for the information system that ○ addresses roles, responsibilities, and configuration management processes and procedures. ○ defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management. ○ establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	✓	

1.6 Contingency Planning (CP)

The following table lists the ITSR related to the CP domain for the EFT Service.

Table C-6: CP Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CP-02	CONTINGENCY PLAN	• The service provider ○ develops a contingency plan for the information system that: ○ Identifies essential missions and business functions and associated contingency requirements; ○ Provides recovery objectives, restoration priorities, and metrics; Addresses contingency roles, responsibilities, and assigned individuals with contact information; ○ Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; ○ Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; ○ Is reviewed and approved by designated officials within the service provider; ○ distributes copies of the contingency plan to key contingency personnel (identified by name and/or by role) and service provider elements.	✓	
CP-02-01	CONTINGENCY PLAN	• The service provider ○ coordinates contingency planning activities with incident handling activities. ○ reviews the contingency plan for the information system at a minimum annually. ○ revises the contingency plan to address changes to the service provider , information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. ○ communicates contingency plan changes to key		✓

ID	Requirement Title	Description	Baseline	Supplemental
		contingency personnel (identified by name and/or by role) and service provider elements. ○ coordinates contingency plan development with service provider elements responsible for related plans. ○ conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. ○ plans for the resumption of essential missions and business functions within a specified time period (as per the contingency plan) upon contigency plan activation. ○ plans for the full resumption of missions and business functions within the time period (stated in the contingency plan) upon contigency plan activation. ○ plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. ○ provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.		
CP-03	CONTINGENCY TRAINING	• The service provider trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at a minimum annually.	✓	
CP-03-01	CONTINGENCY TRAINING	• The service provider incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.		✓
CP-04	CONTINGENCY PLAN TESTING AND EXERCISES	• The service provider tests and/or exercises the contingency plan for the information system using formal tests and/or	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		exercises to determine the plan's effectiveness and the service provider 's readiness to execute the plan at a minimum annually. • The service provider reviews the contingency plan test/exercise results and initiates corrective actions.	✓	
CP-04-01	CONTINGENCY PLAN TESTING AND EXERCISES	• The service provider coordinates contingency plan testing and/or exercises with service provider elements responsible for related plans. • The service provider tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.		✓ ✓
CP-06	ALTERNATE STORAGE SITE	• The service provider establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. • The service provider identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	✓ ✓	
CP-07	ALTERNATE PROCESSING SITE	• The service provider establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period consistent with recovery time objectives when the primary processing capabilities are unavailable. • The service provider identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	✓ ✓	
CP-07-01	ALTERNATE PROCESSING SITE	• The service provider ensures that the alternate processing site provides information security measures equivalent to that of the		✓

ID	Requirement Title	Description	Baseline	Supplemental
		primary site.		
CP-08	TELECOMMUNICATIONS SERVICES	• The service provider establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within time period (as per the contigency plan) when the primary telecommunications capabilities are unavailable.	✓	
CP-08-01	TELECOMMUNICATIONS SERVICES	• The service provider : (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the service provider 's availability requirements; and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. • The service provider obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. • The service provider obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.		✓ ✓ ✓
CP-09	INFORMATION SYSTEM BACKUP	• The service provider conducts backups of user-level information contained in the information system at a frequency consistent with recovery time and recovery point objectives. • The service provider conducts backups of system-level information contained in the information system at a frequency consistent with recovery time and recovery point objectives. • The service provider conducts backups of information system documentation including security-related documentation	✓ ✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
		system at a frequency consistent with recovery time and recovery point objectives. • The service provider protects the confidentiality and integrity of backup information at the storage location in accordance with the TBS Operational Security Standard on Physical Security • The service provider determines retention periods for essential business information and archived backups. • The service provider tests backup information to verify media reliability and information integrity at a minimum annually.	✓ ✓ ✓	
CP-09-01	INFORMATION SYSTEM BACKUP	• The service provider uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. • The service provider stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system. • The service provider transfers information system backup information to the alternate storage site within a specified time period and transfer rate consistent with the recovery time and recovery point objectives.		✓ ✓ ✓
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	• The service provider provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	✓	
CP-10-01	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	• The information system implements transaction recovery for systems that are transaction-based. • The service provider provides the capability to re-image information system components within the restoration time-period(s) from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.		✓ ✓ ✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The service provider protects backup and restoration hardware, firmware, and software.		

1.7 Identification & Authentication (IA)

The following table lists the ITSR related to the IA domain for the EFT Service.

Table C-7: IA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
IA-02	IDENTIFICATION AND AUTHENTICATION (SERVICE PROVIDER USERS)	• The information system uniquely identifies and authenticates service provider users (or processes acting on behalf of service provider users).	✓	
IA-02-01	IDENTIFICATION AND AUTHENTICATION (SERVICE PROVIDER USERS)	• The information system uses replay-resistant authentication mechanisms for network access to privileged accounts and non-privileged accounts. • The information system uses multifactor authentication for remote access to privileged accounts.		✓ ✓
IA-03	DEVICE IDENTIFICATION AND AUTHENTICATION	• The information system uniquely identifies and authenticates all devices before establishing a connection.	✓	
IA-03-01	DEVICE IDENTIFICATION AND AUTHENTICATION	• The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. • The service provider standardizes, with regard to dynamic address allocation, DHCP lease information and the time assigned to devices, and audits lease information when assigned to a device.		✓ ✓
IA-04	IDENTIFIER MANAGEMENT	• The service provider manages information system identifiers for users and devices by ○ receiving authorization from a designated service provider official to assign a user or device identifier. ○ selecting an identifier that uniquely identifies an individual or device.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ assigning the user identifier to the intended party or the device identifier to the intended device. ○ preventing reuse of user or device identifiers for predifined time period (system configurable). ○ disabling the user identifier after time period (system configurable parameter) of inactivity.		
IA-04-01	IDENTIFIER MANAGEMENT	• The service provider ○ prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address). ○ requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority. ○ requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority. ○ manages user identifiers by uniquely identifying the user.		✓
IA-05	AUTHENTICATOR MANAGEMENT	• The service provider manages information system authenticators for users and devices by ○ verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator. ○ establishing initial authenticator content for authenticators defined by the service provider . ○ ensuring that authenticators have sufficient strength of mechanism for their intended use. ○ establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		○ changing default content of authenticators upon information system installation. ○ establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate). ○ changing/refreshing authenticators time period (a system configurable value) by authenticator type. ○ protecting authenticator content from unauthorized disclosure and modification. ○ requiring users to take, and having devices implement, specific measures to safeguard authenticators.		
IA-05-01	AUTHENTICATOR MANAGEMENT	• The information system, for password-based authentication: (a) Enforces minimum password complexity requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type; (b) Enforces at least a number of changed characters when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of numbers for lifetime minimum, lifetime maximum; and (e) Prohibits password reuse for a number of generations. • The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. • The service provider ○ requires that the registration process to receive		✓ ✓ ✓

ID	Requirement Title	Description	Baseline	Supplemental
		types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated service provider official (e.g., a supervisor). ○ protects authenticators commensurate with the sensitivity and criticality of the information and information system being accessed. ○ ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. ○ takes measures to manage the risk of compromise due to individuals having accounts on multiple information systems.		
IA-06	AUTHENTICATOR FEEDBACK	• The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	✓	
IA-07	CRYPTOGRAPHIC MODULE AUTHENTICATION	• The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable CSEC guidance for such authentication.	✓	
IA-08	IDENTIFICATION AND AUTHENTICATION (NON-SERVICE PROVIDER USERS)	• The information system uniquely identifies and authenticates non-service provider users (or processes acting on behalf of non-service provider users).	✓	

1.8 Incident Response (IR)

The following table lists the ITSR related to the IR domain for the EFT Service.

Table C-8: IR Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
IR-02	INCIDENT RESPONSE TRAINING	• The service provider trains personnel in their incident response roles and responsibilities with respect to the information system. • The service provider provides refresher training at a minimum annually.	✓ ✓	
IR-02-01	INCIDENT RESPONSE TRAINING	• The service provider incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.		✓
IR-03	INCIDENT RESPONSE TESTING AND EXERCISES	• The service provider tests and/or exercises the incident response capability for the information system using tests and/or exercises to determine the incident response effectiveness and documents the results at a minimum annually.	✓	
IR-04	INCIDENT HANDLING	• The service provider implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. • The service provider coordinates incident handling activities with contingency planning activities. • The service provider incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	✓ ✓ ✓	
IR-04-01	INCIDENT HANDLING	• The service provider identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of service provider missions and business		✓

ID	Requirement Title	Description	Baseline	Supplemental
		functions. • The service provider correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.		✓
IR-05	INCIDENT MONITORING	The service provider tracks and documents information system security incidents.	✓	
IR-06	INCIDENT REPORTING	• The service provider requires personnel to report suspected security incidents to the service provider incident response capability within THREE (3) months of the incident. • The service provider reports security incident information to designated authorities. • The service provider reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate service provider officials.	✓ ✓ ✓	
IR-07	INCIDENT RESPONSE ASSISTANCE	The service provider provides an incident response support resource, integral to the service provider incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	✓	
IR-08	INCIDENT RESPONSE PLAN	• The service provider develops an incident response plan that: (a) Provides The service provider with a roadmap for implementing its incident response capability; (b) Describes the structure and organization of the incident response capability; (c) Provides a high-level approach for how the incident response capability fits into the overall organization; (d) Meets the unique requirements of the service provider , which relate to mission, size, structure, and functions; (e) Defines reportable incidents;	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		(f) Provides metrics for measuring the incident response capability within the service provider ; (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and (h) Is reviewed and approved by designated officials within the service provider . • The service provider ○ distributes copies of the incident response plan to incident response personnel (identified by name and/or by role) and service provider elements. ○ at a minimum annually reviews the incident response plan. ○ revises the incident response plan to address system/service provider changes or problems encountered during plan implementation, execution, or testing. ○ communicates incident response plan changes to incident response personnel identified by name and/or by role and service provider elements.	✓	

1.9 System Maintenance (MA)

The following table lists the ITSR related to the MA domain for the EFT Service.

Table C-9: MA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
MA-02	CONTROLLED MAINTENANCE	• The service provider ○ schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or service provider specifications and/or service provider requirements. ○ controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. ○ requires that a designated official explicitly approve the removal of the information system or system components from service provider facilities for off-site maintenance or repairs. ○ sanitizes equipment to remove all information from associated media prior to removal from service provider facilities for off-site maintenance or repairs. ○ checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	✓	
MA-02-01	CONTROLLED MAINTENANCE	• The service provider maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (d) Name of escort, if necessary; (e) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).		✓
MA-03	MAINTENANCE TOOLS	• The service provider approves, controls, monitors the use of, and maintains on an ongoing basis, information system	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		maintenance tools.		
MA-03-01	MAINTENANCE TOOLS	• The service provider checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.		✓
MA-04	NON-LOCAL MAINTENANCE	• The service provider authorizes, monitors, and controls non-local maintenance and diagnostic activities. • The service provider allows the use of non-local maintenance and diagnostic tools only as consistent with service provider policy and documented in the security plan for the information system. • The service provider employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. • The service provider maintains records for non-local maintenance and diagnostic activities.	✓ ✓ ✓ ✓	
MA-04-01	NON-LOCAL MAINTENANCE	• The service provider audits non-local maintenance and diagnostic sessions and designated service provider personnel review the maintenance records of the sessions. • The service provider documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections. • The service provider : (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to service provider information) before removal from service provider facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially		✓ ✓ ✓

ID	Requirement Title	Description	Baseline	Supplemental
		malicious software and surreptitious implants) before reconnecting the component to the information system. • The service provider protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either: (a) Physically separated communications paths; or (b) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13. • The service provider requires that: (a) Maintenance personnel notify when non-local maintenance is planned (i.e., date/time); and (b) A designated service provider official with specific information security/information system knowledge approves the non-local maintenance. • The service provider employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.		✓ ✓ ✓
MA-05	MAINTENANCE PERSONNEL	• The service provider ○ establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel. ○ ensures that personnel performing maintenance on the information system have required access authorizations or designates service provider personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	✓	
MA-05-01	MAINTENANCE PERSONNEL	• The service provider maintains procedures for the use of maintenance personnel that lack appropriate security		✓

ID	Requirement Title	Description	Baseline	Supplemental
		clearances or are not Canadian citizens, that include the following requirements: (a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved service provider personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; (b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and (c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.		
MA-06	TIMELY MAINTENANCE	• The service provider obtains maintenance support and/or spare parts for security-critical information system components and/or key information technology components within a time period (noted in continuity plan) of failure.	✓	

1.10 Media Protection (MP)

The following table lists the ITSR related to the MP domain for the EFT Service.

Table C-10: MP Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
MP-02	MEDIA ACCESS	• The service provider restricts access to digital and non-digital media to authorized individuals using security measures.	✓	
MP-02-01	MEDIA ACCESS	• The service provider employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. • The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.		✓ ✓
MP-03	MEDIA MARKING	• The service provider marks, in accordance with service provider policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. • The service provider exempts removable media from marking as long as the exempted items remain within controlled areas.	✓ ✓	
MP-04	MEDIA STORAGE	• The service provider physically controls and securely stores types of digital and non-digital media within controlled areas and in accordance with the RCMP G1-001, Security Equipment Guide • The service provider physically protects and securely stores Classified and Protected information system media awaiting destruction (either on- or off-site) using approved equipment, techniques, and procedures.	✓ ✓	
MP-04-01	MEDIA STORAGE	• The service provider employs cryptographic mechanisms to protect information in storage.		✓

ID	Requirement Title	Description	Baseline	Supplemental
MP-05	MEDIA TRANSPORT	• The service provider protects and controls digital and non-digital media during transport outside of controlled areas using security measures in accordance with the TBS Operational Security Standard on Physical Security and the RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets. • The service provider maintains accountability for information system media during transport outside of controlled areas. • The service provider restricts the activities associated with transport of such media to authorized personnel.	✓ ✓ ✓	
MP-05-01	MEDIA TRANSPORT	• The service provider documents activities associated with the transport of information system media. • The service provider employs cryptographic mechanisms compliant with the requirements of control SC-13 to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		✓ ✓
MP-06	MEDIA SANITIZATION	• The service provider sanitizes information system media, both digital and non-digital, prior to disposal, release out of service provider control, or release for reuse. • The service provider employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	✓ ✓	
MP-06-01	MEDIA SANITIZATION	• The service provider tracks, documents, and verifies media sanitization and disposal actions. • The service provider tests sanitization equipment and procedures to verify correct performance at a minimum annually. • The service provider sanitizes information system media containing sensitive information in accordance with applicable GC policies, standards, and procedures. • The service provider destroys information system media that cannot be sanitized.		✓ ✓ ✓ ✓

1.11 Physical & Environmental (PE)

The following table lists the ITSR related to the PE domain for the EFT Service.

Table C-11: PE Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PE-02	PHYSICAL ACCESS AUTHORIZATIONS	• The service provider develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). • The service provider issues authorization credentials. • The service provider reviews and approves the access list and authorization credentials, removing from the access list personnel no longer requiring access at a minimum annually.	✓ ✓ ✓	
PE-02-01	PHYSICAL ACCESS AUTHORIZATIONS	• The service provider authorizes physical access to the facility where the information system resides based on position or role. • The service provider issues an identification card to all personnel, which as a minimum includes the name of the service provider , the bearer's name and photo, a unique card number and an expiry date.		✓ ✓
PE-03	PHYSICAL ACCESS CONTROL	• The service provider controls access to areas officially designated as publicly accessible in accordance with the service provider 's assessment of risk. • The service provider secures keys, combinations, and other physical access devices. • The service provider inventories physical access devices at a minimum annually. • The service provider changes combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated at a minimum annually. • The service provider enforces physical access authorizations to the information system independent of the physical access controls for the facility.	✓ ✓ ✓ ✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
PE-03-01	PHYSICAL ACCESS CONTROL	• The service provider enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible). • The service provider verifies individual access authorizations before granting access to the facility. • The service provider controls entry to the facility containing the information system using physical access devices and/or guards. • The service provider guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week. • The service provider uses lockable physical casings to protect information system components from unauthorized physical access.		✓ ✓ ✓ ✓ ✓
PE-04	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The service provider controls physical access to information system distribution and transmission lines within service provider facilities.	✓	
PE-05	ACCESS CONTROL FOR OUTPUT DEVICES	The service provider controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	✓	
PE-06	MONITORING PHYSICAL ACCESS	• The service provider monitors physical access to the information system to detect and respond to physical security incidents. • The service provider reviews physical access logs at a minimum annually. • The service provider coordinates results of reviews and investigations with the service provider ’s incident response capability.	✓ ✓ ✓	
PE-06-01	MONITORING PHYSICAL ACCESS	• The service provider monitors real-time physical intrusion alarms and surveillance equipment.		✓

ID	Requirement Title	Description	Baseline	Supplemental
PE-07	VISITOR CONTROL	• The service provider controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	✓	
PE-07-01	VISITOR CONTROL	• The service provider escorts visitors and monitors visitor activity, when required.		✓
PE-08	ACCESS RECORDS	• The service provider maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). • The service provider reviews visitor access records at a minimum annually.	✓ ✓	
PE-08-01	ACCESS RECORDS	• The service provider maintains a record of all physical access, both visitor and authorized individuals.		✓
PE-09	POWER EQUIPMENT AND POWER CABLING	The service provider protects power equipment and power cabling for the information system from damage and destruction.	✓	
PE-10	EMERGENCY SHUTOFF	• The service provider provides the capability of shutting off power to the information system or individual system components in emergency situations • The service provider places emergency shutoff switches or devices in location by information system or system component to facilitate safe and easy access for personnel. • The service provider protects emergency power shutoff capability from unauthorized activation.	✓ ✓ ✓	
PE-11	EMERGENCY POWER	• The service provider provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
PE-12	EMERGENCY LIGHTING	• The service provider employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	✓	
PE-13	FIRE PROTECTION	• The service provider employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	✓	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	• The service provider maintains temperature and humidity levels within the facility where the information system resides at of acceptable levels.	✓	
PE-14-01	TEMPERATURE AND HUMIDITY CONTROLS	• The service provider employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.		✓
PE-15	WATER DAMAGE PROTECTION	• The service provider protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	✓	
PE-16	DELIVERY AND REMOVAL	• The service provider authorizes, monitors, and controls types of information system components entering and exiting the facility and maintains records of those items.	✓	
PE-17	ALTERNATE WORK SITE	• The service provider ○ employs management, operational, and technical information system security controls at alternate work sites. ○ assesses the effectiveness of security controls at alternate work sites. ○ provides a means for employees to communicate with information security personnel in case of security incidents or problems.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	The service provider positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	✓	

1.12 Security Planning (PL)

The following table lists the ITSR related to the PL domain for the EFT Service.

Table C-12: PL Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PL-02	SYSTEM SECURITY PLAN	• The service provider develops a security plan for the information system that: (a) Is consistent with the organization's enterprise architecture; (b) Explicitly defines the authorization boundary for the system; (c) Describes the operational context of the information system in terms of missions and business processes; (d) Provides the security categorization of the information system including supporting rationale; (e) Describes the operational environment for the information system; (f) Describes relationships with or connections to other information systems; (g) Provides an overview of the security control requirements for the system; (h) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and (i) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. • The service provider reviews the security plan for the information system at a minimum annually. • The service provider updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	✓ ✓ ✓	
PL-02-01	SYSTEM SECURITY PLAN	• The organization: (a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: ○ (i) the purpose of the system; ○ (ii) a description of the system architecture;		✓

ID	Requirement Title	Description	Baseline	Supplemental
		○ (iii) the security authorization schedule; and ○ (iv) the security categorization and associated factors considered in determining the categorization; and (b) Reviews and updates the CONOPS as required. • The service provider develops a functional architecture for the information system that identifies and maintains: (a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; (b) User roles and the access privileges assigned to each role; (c) Unique security control requirements; (d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable GC legislation and TBS policies, directives and standards; and (e) Restoration priority of information or information system services.		✓
PL-04	RULES OF BEHAVIOUR	• The service provider ○ establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behaviour with regard to information and information system usage. ○ receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behaviour, before authorizing access to information and the information system. ○ includes in the rules of behaviour, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.	✓	
PL-06	SECURITY-RELATED ACTIVITY PLANNING	• The service provider plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on service provider operations (i.e., mission, functions, image, and reputation), service provider assets, and individuals.	✓	

1.13 Risk Assessment (RA)

The following table lists the ITSR related to the RA domain for the EFT Service.

Table C-13: RA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
RA-02	SECURITY CATEGORIZATION	• The service provider categorizes information and the information system in accordance with applicable GC legislation and TBS policies, directives, and standards. • The service provider documents the security categorization results (including supporting rationale) in the security plan for the information system. • The service provider ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	✓ ✓ ✓	
RA-03	RISK ASSESSMENT	• The service provider conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, in accordance with the TBS Security Organization and Administration Standard • The service provider updates the risk assessment or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system at a minimum annually.	✓ ✓	
RA-05	VULNERABILITY SCANNING	• The service provider scans for vulnerabilities in the information system and hosted applications in accordance with organization-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The service provider employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) Enumerating platforms, software flaws, and improper configurations; (b) Formatting and making transparent, checklists and test procedures; and (c) Measuring vulnerability impact. • The service provider analyzes vulnerability scan reports and results from security control assessments. • The service provider remediates legitimate vulnerabilities in accordance with an service provider assessment of risk. • The service provider shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the service provider to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	✓ ✓ ✓ ✓	
RA-05-01	VULNERABILITY SCANNING	• The service provider employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. • The service provider updates the list of information system vulnerabilities scanned or when new vulnerabilities are identified and reported at a minimum annually.		✓ ✓

1.14 System & Services Acquisition (SA)

The following table lists the ITSR related to the SA domain for the EFT Service.

Table C-14: SA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SA-02	ALLOCATION OF RESOURCES	• The service provider includes a determination of information security control requirements for the information system in mission/business process planning. • The service provider determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process. • The service provider establishes a discrete line item for information security in service provider programming and budgeting documentation.	✓ ✓ ✓	
SA-03	LIFE CYCLE SUPPORT	• The service provider manages the information system using a system development life cycle methodology that includes information security considerations. • The service provider defines and documents information system security roles and responsibilities throughout the system development life cycle. • The service provider identifies individuals having information system security roles and responsibilities.	✓ ✓ ✓	
SA-04	ACQUISITIONS	• The service provider includes security functional requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable GC legislation and TBS policies, directives and standards. • The service provider includes security-related documentation, requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with the TBS Security and Contracting Management Standard • The service provider includes the development and	✓ ✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
		evaluation-related requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable GC legislation and TBS policies, directives and standards.		
SA-04-01	ACQUISITIONS	• The service provider requires in acquisition documents that vendors/service providers provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. • The service provider requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.		✓ ✓
SA-05	INFORMATION SYSTEM DOCUMENTATION	• The service provider obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: ○ Secure configuration, installation, and operation of the information system; ○ Effective use and maintenance of security features/functions; ○ Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. ○ User-accessible security features/functions and how to effectively use those security features/functions; ○ Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; ○ User responsibilities in maintaining the security of the information and information system.	✓	
SA-06	SOFTWARE USAGE	• The service provider uses software and associated	✓	

ID	Requirement Title	Description	Baseline	Supplemental
	RESTRICTIONS	documentation in accordance with contract agreements and copyright laws.		
SA-07	USER-INSTALLED SOFTWARE	• The service provider enforces explicit rules governing the installation of software by users.	✓	
SA-08	SECURITY ENGINEERING PRINCIPLES	• The service provider applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	✓	
SA-09	EXTERNAL INFORMATION SYSTEM SERVICES	• The service provider ○ requires that providers of external information system services comply with service provider information security control requirements and employ appropriate security controls in accordance with the TBS Security and Contracting Management Standard ○ defines and documents government oversight and user roles and responsibilities with regard to external information system services. ○ monitors security control compliance by external service providers.	✓	
SA-09-01	EXTERNAL INFORMATION SYSTEM SERVICES	• The service provider : (a) Conducts an service provider assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by senior service provider official.		✓

1.15 Security Function Isolation (SC)

The following table lists the ITSR related to the SC domain for the EFT Service.

Table C-15: SC Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SC-02	APPLICATION PARTITIONING	• The information system separates user functionality (including user interface services) from information system management functionality.	✓	
SC-02-01	APPLICATION PARTITIONING	• The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.		✓
SC-05	DENIAL OF SERVICE PROTECTION	• The information system protects against or limits the effects of the various types of denial of service attacks.	✓	
SC-05-01	DENIAL OF SERVICE PROTECTION	• The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		✓
SC-07	BOUNDARY PROTECTION	• The information system ○ monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. ○ connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an service provider security architecture.	✓	
SC-07-01	BOUNDARY PROTECTION	• The service provider ○ physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces. ○ limits the number of access points to the information		✓

ID	Requirement Title	Description	Baseline	Supplemental
		system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. ○ Implements a managed interface for each external telecommunication service; ○ Establishes a traffic flow policy for each managed interface; ○ Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; ○ Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; ○ reviews exceptions to the traffic flow policy at a minimum annually; ○ removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. ○ prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. ○ isolates information security tools, mechanisms, and support components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. • The information system ○ fails securely in the event of an operational failure of a boundary protection device. ○ at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems. ○ checks incoming communications to ensure that the communications are coming from an authorized		✓

ID	Requirement Title	Description	Baseline	Supplemental
		source and routed to an authorized destination. ○ implements host-based boundary protection mechanisms for servers, workstations, and mobile devices. ○ prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. ○ routes internal communications traffic to external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. ○ at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). ○ prevents public access into the service provider 's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.		
SC-08	TRANSMISSION INTEGRITY	• The information system protects the integrity of transmitted information.	✓	
SC-08-01	TRANSMISSION INTEGRITY	• The service provider employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The cryptography must be compliant with the requirements of control SC-13.		✓
SC-09	TRANSMISSION CONFIDENTIALITY	• The information system protects the confidentiality of transmitted information.	✓	
SC-09-01	TRANSMISSION	• The service provider employs cryptographic mechanisms to		✓

ID	Requirement Title	Description	Baseline	Supplemental
	CONFIDENTIALITY	prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. The cryptography must be compliant with the requirements of control SC-13.		
SC- 10	NETWORK DISCONNECT	• The information system terminates the network connection associated with a communications session at the end of the session or after a system configurable time period of inactivity.	✓	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	• The service provider establishes and manages cryptographic keys for required cryptography employed within the information system.	✓	
SC-12-01	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	• The service provider maintains availability of information in the event of the loss of cryptographic keys by users.		✓
SC-13	USE OF CRYPTOGRAPHY	• The information system implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.	✓	
SC-13-01	USE OF CRYPTOGRAPHY	• The service provider employs CMVP-validated; CSEC-approved cryptography to implement digital signatures.		✓
SC-14	PUBLIC ACCESS PROTECTIONS	• The information system protects the integrity and availability of publicly available information and applications.	✓	
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	• The service provider issues public key certificates under a certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
SC-19	VOICE OVER INTERNET PROTOCOL	• The service provider ○ establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously. ○ authorizes, monitors, and controls the use of VoIP within the information system.	✓	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	✓	
SC-23	SESSION AUTHENTICITY	• The information system provides mechanisms to protect the authenticity of communications sessions.	✓	
SC-23-01	SESSION AUTHENTICITY	• The information system ○ invalidates session identifiers upon user logout or other session termination. ○ provides a readily observable logout capability whenever authentication is used to gain access to web pages. ○ generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. ○ generates unique session identifiers with radomly.		✓
SC-28	PROTECTION OF INFORMATION AT REST	The information system protects the confidentiality and integrity of information at rest.	✓	

1.16 System & Information Integrity (SI)

The following table lists the ITSR related to the SI domain for the EFT Service.

Table C-16: SI Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SI-02	FLAW REMEDIATION	• The service provider identifies, reports, and corrects information system flaws.	✓	
SI-03	MALICIOUS CODE PROTECTION	• The service provider employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or (b) Inserted through the exploitation of information system vulnerabilities. • The service provider updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with service provider configuration management policy and procedures. • The service provider configures malicious code protection mechanisms to: (a) Perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with service provider security policy; and (b) ☒ block malicious code ☒ quarantine malicious code ☒ send alert to administrator in response to malicious code detection. • The service provider addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	✓ ✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
			✓	

SI-03-01	MALICIOUS CODE PROTECTION	• The service provider
		  ○ centrally manages malicious code protection mechanisms.
		  ○ does not allow users to introduce removable media into the information system.
		  ○ tests malicious code protection mechanisms by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required at a minimum annually.
		• The information system
		  ○ automatically updates malicious code protection mechanisms (including signature definitions).
		  ○ prevents non-privileged users from circumventing malicious code protection capabilities.
		  ○ updates malicious code protection mechanisms only when directed by a privileged user.
				✓
				
				✓

SI-04	INFORMATION SYSTEM MONITORING	• The service provider
		  ○ monitors events on the information system in accordance with monitoring objectives and detects information system attacks.
		  ○ identifies unauthorized use of the information system.
		  ○ deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the service provider .
		  ○ heightens the level of information system monitoring activity whenever there is an indication of increased risk to service provider operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information,
			✓	

ID	Requirement Title	Description	Baseline	Supplemental
		or other credible sources of information. ○ obtains legal opinion with regard to information system monitoring activities in accordance with GC legislation and TBS policies, directives and standards. ○ employs tools to support near real-time analysis of events. ○ protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion. ○ tests/exercises intrusion monitoring tools at a minimum annually. ○ makes provisions so that encrypted traffic is visible to information system monitoring tools. ○ analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. ○ employs mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications of inappropriate or unusual activities that trigger alerts. ○ Analyzes communications traffic/event patterns for the information system; ○ Develops profiles representing common traffic patterns and/or events; ○ Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to and the number of false negatives. ○ employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. ○ employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.		

ID	Requirement Title	Description	Baseline	Supplemental
		• The information system ○ monitors inbound and outbound communications for unusual or unauthorized activities or conditions. ○ provides near real-time alerts when the indications of compromise or potential compromise occur. ○ prevents non-privileged users from circumventing intrusion detection and prevention capabilities. ○ notifies incident response personnel (identified by name and/or by role of suspicious events and takes least-disruptive actions to terminate suspicious events.	✓	
SI-05	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	• The service provider ○ receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. ○ generates internal security alerts, advisories, and directives as deemed necessary. ○ disseminates security alerts, advisories, and directives to personnel identified by name and/or by role . ○ implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of non-compliance.	✓	
SI-07	SOFTWARE AND INFORMATION INTEGRITY	• The information system detects unauthorized changes to software and information.	✓	
SI-07-01	SOFTWARE AND INFORMATION INTEGRITY	• The service provider ○ reassesses the integrity of software and information by performing integrity scans of the information system at a minimum annually. ○ employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. ○ employs centrally managed integrity verification tools. • The service provider requires use of tamper-evident packaging for information system components during		✓ ✓

ID	Requirement Title	Description	Baseline	Supplemental
		☒ transportation from service provider to operational site ☒ during operation		

SI-08	SPAM PROTECTION	• The service provider
		  ○ employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.
		  ○ updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with service provider configuration management policy and procedures.
			✓	

SI-08-01	SPAM PROTECTION	• The service provider centrally manages spam protection mechanisms. • The information system automatically updates spam protection mechanisms (including signature definitions).		✓ ✓
SI-09	INFORMATION INPUT RESTRICTIONS	• The service provider restricts the capability to input information to the information system to authorized personnel.	✓	
SI-10	INFORMATION INPUT VALIDATION	• The information system checks the validity of information inputs.	✓	

SI-11	ERROR HANDLING	• The information system
		  ○ identifies potentially security-relevant error conditions.
		  ○ generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.
		  ○ reveals error messages only to authorized personnel.
			✓	

SI-12	INFORMATION OUTPUT	The service provider handles and retains both information within	✓	

ID	Requirement Title	Description	Baseline	Supplemental
	HANDLING AND RETENTION	and output from the information system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.		

1.17 Awareness & Training (AT)

The following table lists the ITSR related to the AT domain for the EFT Service.

Table C-17: AT Requirements List

ID	Requirement Title	Description	Baseline	Enhancment
AT-02	SECURITY AWARENESS	The service provider provides basic security awareness training to all information system users (including managers, senior executives, and service providers) as part of initial training for new users, when required by system changes, and as a minimum annually thereafter.	✓	
AT-03	SECURITY TRAINING	The service provider provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) As a minimum annually thereafter.	✓	
AT-04	SECURITY TRAINING RECORDS	• The service provider o documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. o retains individual training records for a time period as per service provider internal training policy.	✓	

1.18 Personnel Security (PS)

The following table lists the ITSR related to the PS domain for the EFT Service.

Table C-18: PS Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PS-03	PERSONNEL SCREENING	• The service provider screens individuals prior to authorizing access to the information system in accordance with the TBS Personnel Security Standard • The service provider rescreens individuals according to conditions requiring rescreening.	✓ ✓	
PS-04	PERSONNEL TERMINATION	• The service provider , upon termination of individual employment terminates information system access. • The service provider , upon termination of individual employment conducts exit interviews. • The service provider , upon termination of individual employment retrieves all security-related service provider information system-related property.	✓	
PS-06	ACCESS AGREEMENTS	• The service provider ensures that individuals requiring access to service provider information and information systems sign appropriate access agreements prior to being granted access. • The service provider reviews/updates the access agreements at a minimum annually.	✓ ✓	
PS-06-01	ACCESS AGREEMENTS	• The service provider ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (a) Satisfy associated personnel security criteria.		✓
PS-07	THIRD-PARTY PERSONNEL	• The service provider establishes personnel security control	✓	

ID	Requirement Title	Description	Baseline	Supplemental
	SECURITY	requirements including security roles and responsibilities for third-party providers. • The service provider documents personnel security control requirements. • The service provider monitors provider compliance. • The service provider ensures security screening of private sector organizations and individuals who have access to Protected and Classified information and assets, in accordance with the TBS Personnel Security Standard • The service provider explicitly defines government oversight and end-user roles and responsibilities relative to third-party provided services in accordance with the TBS Security and Contracting Management Standard	✓ ✓ ✓ ✓	
PS-08	PERSONNEL SANCTIONS	• The service provider employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	✓	