Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

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

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

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

Comments - Commentaires

Title - Sujet
PAD-PRE-AUTHORIZED DEBIT RECEIPTS

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

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

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

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

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

Time Zone
Fuseau horaire
Eastern Standard Time
EST

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

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

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

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

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

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

Canada

TABLE 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, Financial and Other 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, Code of Conduct Certifications - Certifications Required Precedent to Contract Award and Additional 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 primary objective is to provide a single service provider, hereafter referred to as Contractor, to process all Pre-Authorized Debit (PADs) in Canadian funds on behalf of Canada. A PAD is a transaction initiated by a government department or agency to commence pre-authorized deductions for fixed or variable amounts, on a recurring or sporadic basis, directly from a payor's bank account. PADs are authorized through written or electronic agreements between the payor and the initiating government department or agency.

2.2 The services are to be delivered nationwide and are required from date of contract to March 31, 2016, with an irrevocable option on the part of Canada to extend the period of the Contract by (2) two additional (1) one year period and (1) one additional (4) four months transition period.

2.3 There is a security requirement associated with this requirement. Please refer to:

- article 1., Security Requirement, of Part 6, Security, Financial and Other Requirements;
- article 3., Security Requirement, of Part 7, Resulting Contract Clauses;
- Annex C, Security Requirements Checklist and its associated attachments.

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 (2012-11-09), Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

The text under Subsection 4 of Section 01 - Code of Conduct and Certifications - Bid of 2003 referenced above is replaced by:

Bidders should provide, with their bid or promptly thereafter, a complete list of names of all individuals who are currently directors of the Bidder. If such a list has not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to provide such a list within the required time frame will render the bid non-responsive. Bidders must always submit the list of directors before contract award.

Canada may, at any time, request that a Bidder provide properly completed and Signed Consent Forms (Consent to a Criminal Record Verification form - PWGSC-TPSGC 229) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/formulaire-forms-eng.html) for any or all individuals named in the aforementioned list within a specified delay. Failure to provide such Consent Forms within the delay will result in the bid being declared non-responsive.

The text under Subsection 5 of Section 01 - Code of Conduct and Certifications of 2003 referenced above is replaced by:

The Bidder must diligently maintain the list up-to-date by informing Canada in writing of any change occurring during the validity period of the bid, and must also provide Canada, when requested, with the corresponding Consent Forms. The Bidder will also be required to diligently maintain the list and when requested, provide Consent Forms during the period of any contract arising from this bid solicitation.

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

Delete: sixty (60) days
Insert: 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(1 hard copies*)*.

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 Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html).

To assist Canada in reaching its objectives, bidders are encouraged to :

1) use paper containing fibre certified as originating from a sustainably-managed forest and/or 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 Goods and Services Tax (GST) or Harmonized Sales Tax (HST) must be shown separately, as applicable.

1.2 Bidders must submit their prices and rates FOB destination; Canadian customs duties and excise taxes included, as applicable; and GST or HST 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

In Section III, Bidders should include the certifications required under Part 5.

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. PAD Transaction Fees
B. Returned Item Transaction Fees

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 items A and B as described below:

A. PAD Transaction Fees:

Firm all-inclusive transaction fee for each debit item included on the PAD file sent from the RG that passes the Contractor's initial edit and is ultimately included in the FI PAD files that are issued to respective Financial Institutions (FIs) for debit from client accounts. This all-inclusive transaction fee must include all processing and reporting requirements.

Instructions

a) Bidders should clearly specify a Firm all-inclusive Fee for each annual volume range and for each year in Tables A1 and A2 (columns B, D, F, I and K).
b) If a bidder wishes to offer a flat fee regardless of volume, they must enter the same fee for each volume range in Tables A1 and A2.
c) The annual Firm all-inclusive fee for PAD transactions will be calculated as: (the arithmetic sum of the Weighted Volume Range Price Factors) * (the annual Forecasted PAD Volumes). This calculation will be completed in Tables A1 and A2.
d) The annual Firm all-inclusive fees for each contract and option year are then summarized in Table A3.

Table A1 - Contract Period

		A	B	C	D	E	F	G
	Annual Volume Range	Weighting Factor	Year 1 Firm All-Inclusive Fees per transaction per Volume Range	Weighted Volume Range Price Factor (A*B)	Year 2 Firm All-Inclusive Fees per transaction per Volume Range	Weighted Volume Range Price Factor (A*D)	Year 3 Firm All-Inclusive Fees per transaction per Volume Range	Weighted Volume Range Price Factor (A*F)
1	**1 – 600,000**	.10	**$**	**$**	**$**	**$**	**$**	$
2	**600,001 – 1,400,000**	.50	**$**	**$**	**$**	**$**	**$**	$
3	**1,400,001 +**	.40	**$**	**$**	**$**	**$**	**$**	**$**
4	Total Weighted Firm All-inclusive Fee per Transaction (rows 1 + 2 + 3)			**$**		**$**		**$**

Table A2 – Option Years

		H	I	J	K	L
	Annual Volume Range	Weighting Factor	Option Year 1 Firm All-Inclusive Fees per transaction per Volume Range	Weighted Volume Range Price Factor (A*B)	Option Year 2 Firm All-Inclusive Fees per transaction per Volume Range	Weighted Volume Range Price Factor (A*D)
1	**1 – 600,000**	.10	**$**	$	$	$
2	**600,001 – 1,400,000**	.50	**$**	$	$	$
3	**1,400,001 +**	.40	**$**	$	$	$
4	Total Weighted Firm All-inclusive Fee per Transaction (rows 1 + 2 + 3)			$		$

Table A3 – Overall total – Summary for Annual Firm All-Inclusive Transaction Fees

ANNUAL FIRM ALL-INCLUSIVE TRANSACTION FEES						
	Category	Year 1	Year 2	Year 3	Option Year 1	Option Year 2
1	Forecasted PAD Volumes	1,170,000	1,320,000	1,410,000	1,520,000	1,560,000
2	Total Weighted Firm All-Inclusive Fee per Transaction (input values from row 4 of Tables A1 and A2)	**$**	**$**	**$**	**$**	**$**
3	**Annual All-inclusive Fee** (rows 1 * 2)	**$**	**$**	**$**	**$**	**$**

B. Returned Item Transaction Fees:

Firm all-inclusive fee for each transaction that is included on the PADR file(s) sent by the Contractor to the RG, including transactions returned to the Contractor from respective FIs as well as transactions rejected in the initial file edits by the Contractor. This Firm all-inclusive fee must include all processing and reporting requirements.

Instructions

a) Bidders should clearly specify a Firm all-inclusive transaction fee for each year in Table B1 (columns A, B, C, D, and E).

Table B1 Annual all-inclusive returned item transaction fees

ANNUAL FIRM ALL-INCLUSIVE RETURNED ITEM TRANSACTION FEES						
		A	B	C	D	E
		Year 1	Year 2	Year 3	Option Year 1	Option Year 2
1	A - Estimated returned item volumes	19,000	22,000	23,000	25,000	26,000
2	B - Transaction fee	$	$	$	$	$
3	**Annual All-Inclusive Fee** (rows 1 *2)	$	$	$	$	$

C. Summary of charges:

Table C1 – 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 All-Inclusive Fee**	**Annual All-Inclusive Fee**	**Annual All-Inclusive Fee**	**Annual All-Inclusive Fee**	**Annual All-Inclusive Fee**
A	**PAD Transaction Fees (Annual all-inclusive fee from Table A3)**	**$**	**$**	**$**	**$**	**$**
B	**Returned Item Transaction Fees (Annual all-inclusive fee from Table B1)**	**$**	**$**	**$**	**$**	**$**
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 Assessed 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 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 Criteria

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

Bids which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

Mandatory Technical Criteria (MT)

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

Number	Mandatory Technical Criterion	Bid Preparation Instructions
MT1	The Bidder must be an Automated Clearing Settlement System (ACSS) direct clearer or ACSS group clearer member having direct clearing membership. The bidder should provide the necessary documentation to support compliance as applicable.	The Bidder should furnish proof of ACSS membership. Membership certificate, membership number or letter of acceptance from the ACSS would be sufficient.
MT2	The Bidder must provide descriptions of 2 projects completed in the past 5 years, whereby the Bidder had processed PADS of at least $850,000 per project	For each project, the Bidder should include the name, title, company, address, email address and telephone number of the contact person along with a brief description of the project that was the basis for the relationship.

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract. Canada will declare a bid non-responsive if the required certifications are not completed and submitted as requested. Bidders should provide the required certifications 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 or to comply with the request of the Contracting Authority for additional information will also render the bid non-responsive.

1. Code of Conduct Certifications - Certifications Required Precedent to Contract Award

1.1 Bidders should provide, with their bid or promptly thereafter, a complete list of names of all individuals who are currently directors of the Bidder. If such a list has not been received by the time the evaluation of bids is completed, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Bidders must submit the list of directors before contract award, failure to provide such a list within the required time frame will render the bid non-responsive.

The Contracting Authority may, at any time, request that a Bidder provide properly completed and Signed Consent Forms (Consent to a Criminal Record Verification form - PWGSC-TPSGC 229) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/formulaires-forms-eng.html) for any or all individuals named in the aforementioned list within a specified delay. Failure to provide such Consent Forms within the delay will result in the bid being declared non-responsive.

2. Additional Certifications Precedent to Contract Award

2.1 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 - over $25,000 and below $200,000

Suppliers who are subject to the Federal Contractors Program (FCP) and have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive federal 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.

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 or more;

d. ( ) 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, in the context of the fee abatement formula, 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 Pension 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

Is the Bidder a FPS in receipt of a pension as defined above ? **YES ( ) NO ( )**

If so, the Bidder must provide the following information:

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

Work Force Reduction Program

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

If so, 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 Goods and Services Tax or Harmonized Sales Tax.

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.

PART 6 - SECURITY AND FINANCIAL REQUIREMENTS

1. Security Requirement

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.

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 PWGSC 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.

2. Financial Capability

SACC Manual clause A9033T(2012-07-16), Financial Capability.

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 Destination of Services

Public Works 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 (2012-07-16), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

The text under Subsection 4 of Section 41 - Code of Conduct and Certifications - Contract of 2035 referenced above is replaced by:

During the entire period of the Contract, the Contractor must diligently update, by written notice to the Contracting Authority, the list of names of all individuals who are directors of the Contractor whenever there is a change. As well, whenever requested by Canada, the Contractor must provide the corresponding Consent Forms.

2.2 Supplemental General Conditions

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

3. Security Requirement

3.1 1. The Contractor must, at all times during the performance of the Contract, 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 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 performed 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 must comply with the provisions of the:

   (a) Security Requirements Check List and security guide (if applicable), attached at Annex C;
   (b) Industrial Security Manual (Latest Edition)

4. Term of Contract

4.1 Period of the Contract

The period of the Contract is from date of Contract to March 31, 2016 inclusive.

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 (2) two additional period of (1) one year 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 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 (4) four 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 (will be identified at contract award)

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 a firm all-inclusive fee as specified in Annex B, Basis of Payment.
Customs duty are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

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 any documents specified in the Contract;
(b) a copy of the invoices, receipts, vouchers for all direct expenses;
(c) total PAD transactions per month
(d) total returned item transactions per month

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 with the certifications 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 or 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

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 _____.

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 (2012-07-16), 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
((i) 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 Databases

12. Insurance

12.1 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. 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 pre-authorized debit (PAD) services and are not to replace any other form of remittances made to the RG, such as cash; cheques; credit or debit cards; electronic funds transfers; or paper or electronic bill payments for which the RG has separate Contracts/arrangements.

A PAD is a transaction initiated by a government department or agency to commence pre-authorized deductions for fixed or variable amounts, on a recurring or sporadic basis, directly from a payor's bank account. PADs are authorized through written or electronic agreements between the payor and the initiating government department or agency.

The framework for processing PADs through the Canadian clearing system is set out in the Canadian Payments Association's (CPA) Rule H1 which outlines the procedures for the processing of PADs. The CPA Automated Clearing Settlement System (ACSS) Rules and Standards mentioned throughout this SOW, including Rules F5, H1, A4 and Standard 005, can be found on the CPA website at the following URL: http://cdnpay.ca/. The Contractor must comply with the CPA rules including any upcoming changes.

There are currently six departments and agencies using the PAD service. Other departments have expressed an interest, but would need to develop the interface between their systems and those of the RG. The current active departments are: Canada Revenue Agency (CRA) for personal and business income tax; Veterans Affairs Canada (VAC) for providing care to long term veterans at St. Anne de Bellevue Hospital; Atlantic Canada Opportunities Agency (ACOA) for their programs; Bank of Canada (BoC) for Canada Savings Bonds; Canadian Economic Development for Quebec Regions (CED) for their programs; and National Defense (DND) for its services. CRA and CED are working on initiatives to expand the use of PADs within the timeframe of the contract period. This was taken into consideration while developing the forecasted volumes provided in *Annex A, Appendix 2 – Historical and Forecasted PAD Activity*.

1.2 Objective

A formal contract is sought with a single service provider, hereafter referred to as the Contractor, to process all PADs in Canadian funds on behalf of Canada.

1.3 Definitions

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

1.3.1 Filenames

i. PAD File: File sent from PWGSC to the Contractor containing a batch of PAD transactions. This file will be in accordance with CPA Standard 005.

ii. PADR File: File sent from the Contractor to PWGSC containing PAD returns received from payor financial institutions (FIs) and/or transactions rejected as part of the Contractor's initial PAD File edits. This file will be in accordance with CPA Standard 005.

iii. FI PAD File: File sent from the Contractor to the direct clearing FIs that will execute the withdrawal instructions. This file contains a batch of PAD transactions and must be in accordance with CPA Standard 005.

iv. FI PADR File: File sent from the direct clearing FIs to the Contractor. This file contains a batch of PAD returns from payor FIs. This file will be in accordance with CPA Standard 005.

1.4 Current Arrangements

There is currently a PAD contract in place with a Canadian FI. The period of the Contract is until March 31, 2013 with an option to extend the contract by a period of 3 months should a transition period by required. .

1.5 Statistical Information

Historical statistics and forecasted volumes are provided in *Annex A, Appendix 2 – Historical and Forecasted PAD Activity*. 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 PAD service.

2.0 DETAILED SERVICE REQUIREMENTS

2.1 General Business Requirements

The Contractor must provide the following services:

i. Accept PAD files in CPA Standard 005 format at the Contractor's data center. The method of delivery of the PAD files is discussed further under the "RG File Exchange" section (2.3), while the timing of the delivery is explained in the "Lead Time" section (2.4).
ii. Perform PAD file edits as outlined in the "Edit and Validation" section (2.6) and process the rejected transactions in accordance with the "Procedure for PAD Rejects" section (2.7).
iii. Sort the valid debit transactions and forward FI PAD files to the direct clearing FIs that will execute the withdrawal instructions (or who will forward these transactions to

the indirect clearing FIs with whom they have a relationship). These files must be sent no later than one business day before the due date to allow debits to occur on the due date. In the event that a PAD file containing transaction(s) with a due date in the past are received by the Contractor, FI PAD files containing these transactions must be sent immediately by the Contractor.

iv. Accept funds from payor FIs for all debit transactions sent.

v. Process PAD returns in accordance with the “Procedure for PAD Returns” section (2.10).

vi. Respond to enquiries from the RG relating to PADs, PAD rejects, and PAD returns within the timeframe set out in the “Traces and Enquiries” section (2.12).

2.2 Enrollment

The enrollment and verification process will be performed by the originating government department or agency in compliance with CPA Rules. It is not the responsibility of the Contractor.

2.3 RG File Exchange

The mandatory method of delivery to transfer files is the CPA’s Service Network (CSN). File transmission, through use of this delivery method, is done by private frame relay for security purposes and is in compliance to all CPA rules/standards (F5, H1, A4, and CPA Standard 005).

The Contractor must periodically review the appropriateness and operation of the methods of delivery and must cooperate in implementing such changes or modifications to standards as may be agreed with the RG. If the standard adopted by the parties is officially changed, or modified by the issue of a new version or release, the Contractor must use its best efforts to agree on a program or schedule to change the instructions and information based on the new standard as promptly as practicable and must cooperate to effect the change in a commercially reasonable manner.

2.4 Lead Time

The RG will typically send the PAD files in advance of the due date in accordance with the serviceability code associated with the payor’s FI, as outlined in the FIF file (4 days or less). It is possible however that some transactions contained in the PAD files will have due dates up to 14 days in the past.

The RG will send the PAD file to the Contractor on each business day by no later than 09:30 EDT, except on days where the RG has no activity. If a delay is experienced, the RG will notify the Contractor’s operational contact of the delay and the expected time of transmission. In the event that problems arise and the file cannot be transmitted, the RG will contact the Contractor and the parties will make mutually agreeable arrangements.

If the Contractor has not received the PAD files from the RG by 09:30 EDT, then the Contractor must contact the RG’s operational contact and inquire about the delay. Alternate arrangements to deliver the PAD will be made, if necessary.

2.5 File Distribution, Processing and Retention of Records

The Contractor must:

i. For tracing purposes, retain all PAD and returned/rejected transactions for a period of one year from the PAD due date.

ii. Include a unique sequentially assigned file creation number for each FI PAD file and PADR File for tracing/reconciliation purposes.

2.6 Edit and Validation

Upon receipt of a file, the Contractor must promptly perform the following edits and validation. Edit and validation must occur on the individual transaction level. The Contractor must reject only those transactions that fail the edits and validation, without the need to reject the entire file.

i. Perform PAD file edits including:
   a) Stale dated transactions (as per the Due Date requirements listed in CPA Standard 005).
   b) Validity of FI number and branch as per financial institution file (FIF) updates provided by CPA.

ii. Perform FI PADR file edits as required including:
   a) Originator other than federal government.
   b) Invalid transaction type (only CPA codes will be accepted).
   c) Duplicate transactions where the original PAD transaction has already been returned.
   d) Invalid transactions where the RG's ITN, RG's PRN and/or amount do not match the original PAD transaction.

2.7 Procedure for PAD Rejects

The Contractor must:

i. Perform PAD file edits as stipulated in the "Edit and Validation" section (2.6)
ii. To initiate settlement for PAD Rejects, the Contractor must complete a notification form, or SWIFT MT299 message, to be sent to the BoC no later than 14:30 EDT. The amount listed in this notification/MT299 is the amount that the BoC will send to the contractor through a LVTS payment. The "Settlement of PADR files" section (2.11.2) contains additional details regarding the settlement of PAD rejects. The required notification form data elements and required MT299 formatting can be found in the "Reject / Return Notification Requirements" section (2.0) of *Annex A, Appendix 3 – Bank of Canada Notification Requirements.*
iii. Return un-posted transactions to PWGSC through a PADR file in accordance with the CPA Standard 005. Each file must include the RG's ITN, PRN, institutional ID number, and a unique file creation number created by the Contractor for tracing/reconciliation purposes. These files must be sent by the Contractor and received by the RG prior to 19:45 EDT on the settlement date. The value of the PADR file(s) must match the amount reported in the notification/MT299 message that was sent to the BoC as per step (ii) of this section.
iv. PAD rejects may be included in a PADR file also containing PAD Returns or reported in a separate PADR file.

2.8 Procedures for Replacement of Electronic File

At the request of the RG, if a file is unreadable, the Contractor must re-create and re-submit a PADR file. This request, if made, must be made within 15 business days of the transmission date of the original file.

The Contractor has no more than 2 business days to re-create or re-submit a PADR file.

2.9 Float

The Contractor must pay float interest to the RG on any funds where the settlement date is later than the date the funds were received by the Contractor from the payor's FI. 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.

2.10 Procedure for PAD Returns

The Contractor must:

i. Comply with CPA rules regarding dishonored PADs for any reason such as, but not limited to, non-sufficient funds (NSF), stop payment, or account closed. Items must be returned within the time limitations set out in Rule A4 and the procedures set out in Rule F5;
ii. Accept PAD returns (FI PADR files) from payor FIs no later than 90 calendar days for personal or funds transfer PADs, and 10 calendar days for business PADs after the posting date on the account statement as stipulated by the CPA rules;
iii. Perform FI PADR file edits as stipulated in the "Edit and Validation" section (2.6);
iv. Comply with CPA Standard 005 for the reject codes, the record type identifier and the record file layout.
v. Complete a notification form, or SWIFT MT299 message, to be sent to the BoC no later than 14:30 EDT. The amount listed in this notification/MT299 is the amount that the BoC will send to the contractor through a LVTS payment. The "Settlement of PADR files" section (2.11.2) contains addition details regarding settlement. The required notification form data elements and required MT299 formatting can be found in the "Reject / Return Notification Requirements" section (2.0) of *Annex A, Appendix 3 – Bank of Canada Notification Requirements.*
vi. PADR file(s) containing all returned transactions must be sent by the Contractor and received by the RG prior to 19h45 EDT on the settlement date. Each file must follow the CPA Standard 005 file layout and must include the RG's ITN, RG's PRN, and a unique file creation number created by the Contractor for tracing/reconciliation purposes. The value of the PADR file(s) must match the amount reported in the notification/MT299 message that was sent to the BoC as per step (v) of this section.
vii. PAD Returns may be included in a PADR file also containing PAD Rejects or reported in a separate PADR file.
viii. Any returns by direct clearers beyond the time limits as stipulated in the CPA rules for returns must be refused by the Contractor on behalf of the RG.

2.11 Settlement

2.11.1 Settlement of PAD Files

i. The Contractor must initiate and send to the BoC before 15:00 EDT on the PAD transaction date a LVTS payment message MT103 in favor of the RG. The required MT103 formatting can be found in the "File Specifications for SWIFT MT103 Message" section (3.0) of *Annex A, Appendix 3 – Bank of Canada Notification Requirements*.
ii. This LVTS payment must be accompanied by either a notification form or SWIFT MT299 message. The amount of the LVTS payment must match the amount reported in the notification/MT299 message. The required notification form elements

and required MT299 formatting can be found in “PAD Notification Requirements” section (1.0) of *Annex A, Appendix 3 – Bank of Canada Notification Requirements.*

iii. The amount of the LVTS payment message MT103 must be for the full value of the PAD File(s). PAD Rejects and Returns should not be deducted from the value of the PAD File(s) as they are settled separately (see the “Procedure for PAD Rejects” section (2.7), and the “Procedure for PAD Returns” section (2.10) for further details on the settlement of PAD Rejects and PAD Returns.)

2.11.2 Settlement of PADR Files

The Bank of Canada (BoC) will initiate and send to the Contractor before 15:00 EDT on the settlement date an LVTS payment message MT103 in favor of the Contractor. The BoC will complete the mandatory fields and indicate *“PAD Return”* in the applicable field. The amount of the LVTS payment initiated by the BoC shall be equal to the amount that the Contractor reported on the notification form/MT299 message described in part (v) of “Procedure for PAD Returns” (section 2.10) or part (ii) of the “Procedure for PAD Rejects” (section 2.7).

2.12 Traces and Enquiries

The Contractor must resolve any enquiries and/or provide clarification of a PAD transaction within 5 business days when requested by the RG. Upon failure to resolve an enquiry within 5 business days, the RG may escalate the enquiry within the Contractor’s organization. All trace requests from the RG will include a PWGSC Original Trace Number; this number must be referenced in all responses.

2.13 Reports

RG will fulfill their own reporting requirements with the PADs and PADRs files received from the Contractor.

2.14 Response Time

For billing inquiries, the Contractor must respond within 7 calendar days. The response time for all other enquiries by the RG shall be 2 hours by phone/e-mail.

3.0 TRANSITIONAL ACTIVITIES

3.1 Implementation of Service

i. Implementation activities must begin within 5 business days after date of Contract award. These activities must include:
   a) Within 3 business days notice from the RG, meetings/conference calls, as required, of high level/operational/technical teams with the RG to ensure an organized implementation process and on-going operations;
   b) A transition plan must be finalized and submitted to the RG within 14 claendar days of date of Contract award;
   c) Transition phase must not take more than 90 days and is to include:
      1. Contractor setup phase (technical requirements)
      2. Edits/formats as stipulated in the SOW
      3. Provide the PAD and PADR transaction details/files as stipulated in the SOW;

4. Testing requirements for transmission of PAD and PADR files with the RG;
5. Availability to test electronic files in a test environment;
6. Once approved by the RG, moving the electronic transmission into production;
7. Provide the RG with a contingency plan for exchange points and time frames;
8. Liaising with the BoC to finalize settlement arrangements;
9. Any other requirements as per the SOW.

ii. The Contractor must, no more than 14 calendar days after date 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, the second and third level escalation contacts as well as 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.

3.2 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 4 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.

4.0 OTHER REQUIREMENTS

4.1 Contingency and Disaster Recovery Plan

As outlined in *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, labor 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 between it and the RG by alternate means that are mutually agreed upon between the parties. Even in a contingency situation, the file format must remain in compliance with the CPA Standard 005.

4.2 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*.

4.3 Language of Service

The Contractor must provide the services in both official languages of Canada, English and French. 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

4.4 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, 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 and LVTS files in this new format.

4.5 Changing of PADR Reporting and Settlement Process during Contract

Due to internal system changes, at some point during the life of this contract, the RG may request a change in the reporting and settlement procedures for PADR transactions. Should these changes be implemented, the Contractor would no longer be required to send a notification form/MT299 message to the Bank of Canada, followed by the transmission of corresponding PADR file(s) to the RG. Instead, the Contractor would simply be required to send PADR file(s) to the RG by 08:30 EDT to receive a same-day payment from the Bank of Canada (in the form of an LVTS payment message MT103).

ANNEX A – APPENDIX 1
DEFINITIONS

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.

Due Date: Date authorized by the payor for the withdrawal of funds from his account.

FIF (Financial Institution File): An electronic directory of the FIs and their branches that is maintained by the CPA.

File Names (PAD File, PADR File, FI PAD File, FI PADR File): Please refer to Annex A, 1.3 Definitions.

File Presentation Date: The banking day that the PAD file is provided to the Contractor.

Frame Relay: A packet-switching protocol for connecting devices on a Wide Area Network (WAN). This type of line connection is used by the CPA Services Network to ensure the maximum security level.

ITN (Item Trace Number): A 22 digit number provided by the RG and included by the Contractor with each transaction in a PAD file. The original ITN is also included with each transaction in a PADR file sent from the Contractor to the RG.

LVTS (Large Value Transfer System): 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.

PADR: Rejected or returned pre-authorized debit transactions.

PAD Transaction Date: Date the funds were debited from the payor's account.

Payor: A person or organization who pre-authorizes the withdrawal of funds directly from their bank account.

PRN: A reference number assigned by the SPS for internal reference for the RG and the originator and is assigned to every PAD transaction.

Reject: A transaction that fails the initial file edits by the Contractor and is returned to the RG.

Return: A transaction returned by the Payor's FI for reasons consistent with CPA rules/standards.

Settlement Date: For settlement of PAD Files, this is the date the RG receives value at the Bank of Canada. For settlement of PADR Files, this is the date that the Contractor receives value for PAD Rejects and PAD Returns.

SPS (Standard Payment System): The treasury system managed by the RG.

SWIFT: Society for Worldwide Interbank Financial Telecommunication.

ANNEX A – APPENDIX 2
HISTORICAL AND FORECASTED PAD ACTIVITY

1.0 Historical PAD Volumes and Values For the 2009/2010 to 2011/2012 Fiscal Years

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

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

2.0 Forecasted Volumes

Contract Period	Transactions	Returns
2013/2014	1,170,000	19,000
2014/2015	1,320,000	22,000
2015/2016	1,410,000	23,000
Option Year 1 2016/2017	1,520,000	25,000
Option Year 2 2017/2018	1,560,000	26,000

ANNEX A – APPENDIX 3
BANK OF CANADA NOTIFICATION REQUIREMENTS

1.0 PAD Notification Requirements

1.1 Required Notification Data Elements for PAD Files

a) Document Title: “PADs – Details of Settlement Value”
b) Financial Institution Name
c) Settlement Date
d) Details of each PAD file included within the settlement. Details of each file must include:
    i. Due Date
    ii. Originators Identification Number
    iii. File Creation Number
    iv. Number of Debit Payments
    v. Payment Amount
e) Total Settlement Value
    i. This value must equal the sum of the Payment Amount of each PAD file listed in (d). It must also equal for the amount of the LVTS payment message MT103 sent to the BoC.
f) Contact Information of Sender.

1.2 File Specifications for SWIFT MT299 Message

SWIFT field code	SWIFT field name	BOC Required Information
20	Client Reference	PAD Settlement
21	Related Reference	Receiver General
32A	Value date, Currency, Settlement Amount	
79	Narrative	ATTN: Payment and Settlement Operations Government PAD Settlement Settlement date: YYYY-MM-DD Details of Settlement Value: i. Due Date ii. Originators Identification Number iii. File Creation Number iv. Number of Debit Payments v. Payment Amount Total Settlement Value: CAD Contact Info Telephone Position

2.0 Reject / Return Notification Requirements

2.1 Required Notification Data Elements for PADR Files

a) Document Title: “PADs – Detail of Rejects and Returns”
b) Financial Institution Name
c) Reject / Return File Presentation Date
d) Details of each PADR file included within the settlement. Details of each file must include:
    i. File Creation Number
    ii. Number of Debit Payments
    iii. Payment Amount
e) Total Reject / Return Value
    i. This value must equal the sum of the Payment Amount of each PADR file listed in (d). This will be the amount that the BoC will send to the Contractor via LVTS on the Reject / Return File Presentation Date.
f) Contact Information of Sender.

2.2 File Specifications for SWIFT MT299 Message

SWIFT field code	SWIFT field name	BOC Required Information
20	Client Reference	PAD Return
21	Related Reference	Receiver General
32A	Value date, Currency, Settlement Amount	
79	Narrative	ATTN: Payment and Settlement Operations Government PAD Return / Reject Settlement date: YYYY-MM-DD Details of Settlement Value: i. File Creation Number ii.Number of Debit Payments iii. Payment Amount Total Return / Reject Value: CAD Contact Info Telephone Position

3.0 File Specifications for SWIFT MT103 Message

SWIFT field code	SWIFT field name	Bank of Canada Required Information
20	Client Reference	Govt PAD
23B	Bank Operation Code	CRED
32A	Value date, Currency, Settlement Amount	
50A	Ordering Customer	BIC of Contractor
57A	Account with Institution	BOC BIC
59	Beneficiary Customer	RG Account No. With BoC Receiver General
72	Bank to Bank Information	/ACC/560: or /BNF/560: or /REC/560:

ANNEX B

BASIS OF PAYMENT

Contract Period: The period of the contract is from date of Contract to March 31, 2016. .

During the period of the Contract, the Contractor will be paid as specified below, for Work performed in accordance with the Contract. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax (GST/HST) is extra, if applicable.

1.0 PAD Transaction Fee

Firm all-inclusive transaction fee for each debit item included on the PAD file sent from the RG that passes the Contractor's initial edit and is ultimately included in the FI PAD files that are issued to respective Financial Institutions (FIs) for debit from client accounts. This all-inclusive transaction fee would include all processing and reporting requirements.

		A	B	C	D	E
	Volumes	Firm All-Inclusive PAD Transaction Fee Year 1	Firm All-Inclusive PAD Transaction Fee Year 2	Firm All-Inclusive PAD Transaction Fee Year 3	Firm All-Inclusive PAD Transaction Fee Option Year 1	Firm All-Inclusive PAD Transaction Fee Option Year 2
1	1 – 600,000	$	$	$	$	$
2	600,001 – 1,400,000	$	$	$	$	$
3	1,400,001 +	$	$	$	$	$

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

2.0 Returned Item Transaction Fee:

Firm all-inclusive fee for each transaction that is included on the PADR file(s) sent by the Contractor to the RG, including transactions returned to the Contractor from respective FIs as well as transactions rejected in the initial file edits by the Contractor. This unit fee will include all processing and reporting requirements.

	Firm All-Inclusive Fee for Year 1	Firm All-Inclusive Fee for Year 2	Firm All-Inclusive Fee for Year 3	Firm All-Inclusive Fee for Option Year 1	Firm All-Inclusive Fee for Option Year 2
Firm All-Inclusive Transaction fee on Returned Item	$	$	$	$	$

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

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

2.2 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
EN891130776
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

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

4. Brief Description of Work / Brève description du travail

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

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

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

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

Government of Canada / Gouvernement du Canada

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

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux : _____

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

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

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

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

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

The Contractor must demonstrate that any IT system(s) and/or application(s) that will be used in the delivery of the PAD service meet the Baseline Requirements identified herein. If applicable to the proposed PAD 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 PAD service meet the Supplemental Requirements.

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 PAD 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 ○ Security Function Isolation ○ System & Information Integrity • The service provider develops, disseminates, and reviews/updates a formal, documented procedures to facilitate the implementation of	✓ ✓	

ID	Requirement Title	Description	Baseline	Supplemental
		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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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 PAD 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.	✓	