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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Prepaid Card Services	
Solicitation No. - N° de l'invitation EN891-130377/B	**Date** 2014-02-17
Client Reference No. - N° de référence du client 20130377	**GETS Ref. No. - N° de réf. de SEAG** PW-$$ZG-419-27182
File No. - N° de dossier 419zg.EN891-130377	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2014-03-31**	**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: McNeely, Lysianne	**Buyer Id - Id de l'acheteur** 419zg
Telephone No. - N° de téléphone (819) 956-5193 ( )	**FAX No. - N° de FAX** (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

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

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

Please see attached Request for Information (RFI).

THIS IS NOT A SOLICITATION DOCUMENT

THIS IS A REQUEST FOR INFROMATION (RFI) FROM INDUSTRY
FOR THE
PREPAID CARD SERVICES

Previous Request for Comments (RFC)

There was a RFC issued on June 18, 2012 and closed on July 19, 2012. The vision and scope of the prepaid card requirement for the Receiver General has changed since the previous RFC.

The intent of this new Request for Information (RFI) is to solicit feedback on all aspects detailed herein and the new draft Statement of Work, draft Mandatory Technical Criteria, and the Security Requirements Checklist (SRCL), and the draft Security and Privacy Requirements so as to enable Canada to evaluate the strategy to be taken, if any, regarding further related activities.

More specifically, feedback is sought regarding:

- The potential level of interest in providing services to address the requirements of the attached Draft Statement of Work;
- The processes and procedures involved with issuing an electronic form of payment for various government programs;
- To obtain information and suggestions on other ways of performing similar functionality or improving on what is being presented; and
- With respect to draft Security and Privacy Requirements document, indicate if your organization's implementation of the capability is the same as described for that specific requirement. If it is not, provide a description of how your organization addressed the specific requirement.

SERVICE REQUIREMENTS

The Receiver General for Canada (RG) plans to begin issuing Prepaid Cards as a new payment product for beneficiaries as a replacement to the paper cheque process wherever possible. The RG aims to contract with a service provider to issue, activate, and load prepaid cards as well as provide support services to Cardholders. Additionally, the RG requires the ability to provide instant issuance prepaid cards as may be required by some departments.

These services may be required for a period of five (5) years commencing from date of Contract with an irrevocable option on the part of Canada to extend the period of any resulting Contract by two (2) additional 1-year periods and one (1) additional twelve (12) month transition period.

There is a security requirement associated with this requirement. Please refer to the Security Requirements Checklist (SRCL) and draft Security and Privacy Requirements, including the following clause which will form part of any resulting Contract:

DRAFT SECURITY REQUIREMENT CLAUSE

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 and an IT Link 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);
(b) Industrial Security Manual (Latest Edition)

Potential service providers who currently **DO NOT MEET** the facility security clearance requirements and (or) personnel security clearance should initiate the security clearance process by requesting sponsorship from the Contracting Authority. For any inquiries concerning any security requirements, suppliers 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/.

NOTE TO POTENTIAL RESPONDENTS

Responses

The material in this RFI package is for the solicitation of **feedback only**. Responding to this RFI is not a prerequisite to receiving any Request for Proposal for the Accounting Banking & Compensation Branch (ABCB) requirement. However, all Respondents are encouraged to indicate their level of interest by responding to this RFI with its comments in order to facilitate a better understanding of requirements and Industry perspectives.

The publication of this RFI must not be construed as a commitment on Canada's part to issue a subsequent "Request for Proposal" for ABCB's requirement and no contract or other form of commitment will be entered into with any Respondent based on responses to this RFI. This RFI must in no way be considered as authorization by Canada for Respondents to undertake any work, which would result in costs to Canada.

Canada will not be liable for, nor will it reimburse any Respondents for any costs, fees or expenses which any Respondent incurs in the preparation or submission of its response to this RFI. Canada will not be bound by anything stated herein. Canada reserves the right to change, at any time, any or all parts of the requirement as it renders necessary.

Respondents are advised that any information submitted to PWGSC in response to this RFI may be used in the development of a subsequent RFP. Respondents will not be bound by any aspect of their response to this RFI. All responses to this RFI will be held by Canada on a confidential basis (subject to applicable legislation), and remain the property of Canada once they have been received and may be used to support further development of internal planning documents and decisions, and possibly an RFP. Note that responses to the RFI will not be returned.

Participation

The RFI is inclusive and flexible and is not intended to pre-qualify Respondents for any stages of the project. An interested Respondent who does not participate in the RFI process is not precluded from participating in any subsequent RFP process.

CLOSING DATE

Responses to this RFI will be accepted until **2:00 PM Eastern Standard Time (EST) on March 31, 2014**. Responses are to be submitted by fax or electronically to the Contracting Authority stated below. The information received after that date will be considered only to the extent reasonable, in the sole opinion of Canada, given the progress of the Work at the time of receipt of the said information.

ENQUIRIES

Any questions from Respondents concerning this RFI must be made in writing to the Contracting Authority stated below, via e-mail on or before the closing date of this RFI.

Respondents are to assume all responsibility for the successful delivery and receipt of all questions to the Contracting Authority stated below. Questions submitted to any other person but the Contracting Authority, or in any other form, will not be answered. Responses given in any other manner than that which is outlined above will not be binding upon any party.

Canada reserves the right not to respond to questions received after the closing date of this RFI, or to any question not related to this RFI. 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 respondent do so, so that the proprietary nature of the question is eliminated, and the responses will be made publicly available through Buy & Sell web site (https://buyandsell.gc.ca/). Enquiries not submitted in a form that can be distributed to all Respondents may not be answered by Canada. If a question is determined to be proprietary, in Canada’s sole discretion, Canada reserves the right to respond only to that party.

CLARIFICATION

PWGSC may require clarification of written responses and/or comments received as a result of the responses to this RFI. If required, any clarification will be requested by the Contracting Authority after the closing date of the RFI. Requests for clarification will be submitted in writing (by email only) and a response will be requested within two (2) working days of transmission of the clarification questions. Canada will not provide any guidance on how to prepare the responses or of any acceptable response strategy.

FORMAT OF RESPONSE

Respondents should review and provide comments to the attached draft documents and respond to the set of questions of below.

RESPONSES REGARDING THIS REQUIREMENT ARE TO BE SUBMITTED TO THE FOLLOWING PWGSC CONTRACTING AUTHORITY:

Lysianne McNeely,
Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Professional Services Procurement Directorate
Place du Portage, Phase III, 10C1
11 Laurier Street
Gatineau, Quebec
K1A 0S5

Tel: (819) 956-5193
Fax: (819) 956-2675
Email: Lysianne.McNeely@tpsgc-pwgsc.gc.ca

Questions to the RFI

The vision of the prepaid card program for the Receiver General has changed since the previous Request for Comments (RFC) issued in 2012. The new Statement of Work and forecasted estimates involve the use of the program by multiple government departments and programs, as well as the availability of instant issuance prepaid cards where required.

Please refer to the attached draft Statement of Work and the Mandatory Evaluation Criteria.

Some of the following questions may be repeated from the previous RFC but due to these changes, as well as advances in the prepaid industry and technology, Canada is requesting the most current answers.

1) Are the requirements as stated in the attached draft Statement of Work (SOW) clear?

2) Please identify any issues that would limit your ability to perform the work outlined in the SOW. In particular, please indicate any areas where it may be difficult to attain service levels (Section 7 of the SOW).

3) Beneficiaries with disabilities are of particular concern for the RG. How do your services (web sites, telephone system) accommodate users with special needs? Do your websites follow the WCAG 2.0 guidelines?

4) The government is envisioning a program where cardholders can use their card without incurring fees wherever possible. Certain fees may be unavoidable (ex: out of network ATM use, foreign exchange), can you provide a list of the other types of fees that may be imposed onto cardholders?

5) Cardholders must be able to use their cards throughout the country. While out of network ATM usage fees may be unavoidable, cardholders must have access to a large number of ATMs that are considered in-network. A minimum number of available in-network ATMs will be specified by the RG. How large is your existing in-network ATM coverage, and would you be willing to partner with other institutions to increase your in-network coverage if necessary?

6) The RG would like cardholders to be able to activate their cards via the web and by telephone. What other activation routes would you propose? How do your activation processes minimize the potential for fraudulent card activation? Exact details of the process can be determined between the RG and the winning bidder. Please note that the SIN will not be available for use in the process.

7) What is the minimum lead time that would be required to make a payment to an account? If the payment file is sent by the RG by 4:00 p.m. on a given day, could the funds be available to the cardholder at start of business the following day?

8) Please explain your preferred method of secure file transmission with the RG.

9) The RG is concerned with the potential for fraud associated with the use of prepaid cards. Please explain how your processes protect against and detect fraud, both for the cardholder and to the RG.

10) In the event that fraudulent activities are detected, what are your processes to notify the affected parties and halt the fraud?

11) The RG expects zero liability to the rightful beneficiary in the event they are affected by fraudulent card activity. Are there any cases where zero liability would not apply?

12) Security of data is important to the RG. Please explain how you would ensure the payment data will be kept secure.

13) Do the provided volumes and forecasts in section 9.1 of the draft SOW provide enough information? As different programs identify beneficiaries differently, Canada is unable to accurately determine cardholder overlap. A likely outcome is that beneficiaries who do receive multiple cards will contact issuing departments to have their benefits consolidated onto a single card.

14) What additional information would you need to be able to fully assess the whole project?

15) Is your firm currently registered in the Industrial Security Program (ISP) of PWGSC's Canadian Industrial Security Directorate? If not, would your firm be interested in registering? If so, please send a request for sponsorship to the Contracting Authority.

16) Would your firm be able to submit a responsive bid based on the attached Mandatory Technical Criteria? If not, please describe the reason(s) why.

17) Would your firm be able to submit a responsive bid based on the draft Security and Privacy Requirements?

18) Would you bid on this requirement if it was tendered as described herein? If not, please describe why.

19) Do you have any other concerns that you would like to address?

STATEMENT OF WORK

FOR

PREPAID CARD

Table of Contents

1 Purpose

The Receiver General for Canada (RG) plans to begin issuing Prepaid Cards as a new payment product for beneficiaries as a replacement to the paper cheque process wherever possible. The RG aims to contract with a service provider to issue, activate, and load prepaid cards as well as provide support services to Cardholders. Additionally, the RG requires the ability to provide instant issuance prepaid cards as may be required by some departments. The purpose of this document is to describe the work requirements for the two prepaid card systems and to solicit bids from service providers.

2 Overview of Prepaid Cards and Instant Issuance Cards

The RG is responsible for issuing payments on behalf of federal government departments and certain provincial governments by using a number of payment products including direct deposits, paper warrants and wire transfers. The federal government is working to phase out its issuance of paper warrants by April 2016. This is being done primarily to reduce costs (i.e.: postage, printing, storage) and improve the reconciliation process. Beneficiaries are being strongly encouraged to enroll in the Direct Deposit program to receive government payments. Those who do not sign up in direct deposit will be gradually enrolled into the prepaid card program by payment issuing departments. Once the April 2016 phase out target date arrives, all beneficiaries still receiving cheques will automatically be switched to prepaid cards unless they qualify for and register as an exception.

Currently, departments and programs are able to issue payment by cheque (“cheque” and “warrant” are considered interchangeable in this document) by using their departmental financial system to send the payment information to the RG’s payment system, the Standard Payment System (SPS). The prepaid card program will involve changes to the SPS such that payment details received from departments identified as cheques will instead be issued as prepaid cards. The SPS will have a system in place to identify beneficiaries across government so that multiple departments and programs are able to issue payments to the same card. One-time and recurring payments will be issued to the same card.

The RG will inform the Contractor of beneficiaries to be enrolled in the prepaid card program and the Contractor will mail out the cards and instructions for activation. Once enrolled, any payment received by the SPS for that beneficiary will be sent to their prepaid card account with the Contractor. On the due date, the Contractor makes the payment to the beneficiary’s prepaid card account, and then makes their claim for settlement.

Additionally, the RG plans to implement a program allowing the instant issuance of prepaid cards for amounts determined by departments as required. In certain circumstances government payments must be issued with very little advance notice. Instant issuance cards must be available to allow departments to assign, activate and load a prepaid card from a departmental location where funds are available to the beneficiary immediately.

Please note that in this document, “prepaid cards” will refer to the cards being used to replace cheque payments while “instant issuance prepaid cards” will refer to only the cards required by certain programs for instant loading and availability of funds.

3 Detailed Requirements

3.1 General Contractor Requirements

3.1.1 Locations

1) The Contractor must provide prepaid cards by mail to all beneficiaries referred by the RG across Canada.
2) The Contractor must provide instant issuance cards to departmental locations specified by the Project Authority.

3.1.2 Language

The Contractor must be capable of providing services in both official languages (English and French). The Help Desk should provide bilingual customer service. Documentation for card recipients and websites to be used by Cardholders must be available in both English and French.

3.1.3 Documentation

1) The Contractor must be able to, upon request, provide bilingual documentation (including but not limited to industry-standard operator manuals and promotional material) that will allow departments and the PA to effectively use the prepaid card program and the instant issuance prepaid card program.
2) All documentation pertaining to the RG's prepaid card program must be provided to the PA for pre-approval.

3.1.4 Sub-Contractors Interface

If the Contractor utilizes sub-contractors, it must provide a concise description of each sub-contractor, including the nature of the business and the location and extent of operations. The PA will have no interaction with the sub-contractor(s).

3.1.5 SPS Interface

For the prepaid card program, multiple interfaces with the SPS will be required. Files will be sent from the SPS to the Contractor for the enrolment of beneficiaries and updating of existing beneficiary data, payment data will be sent to the Contractor, and return files must be sent by the Contractor.

- For beneficiary enrolment refer to section 4.1.2.
- For updating enrolment status refer to section 4.1.3
- For payment load refer to section 4.1.5

A method of secure file transmission will be determined by the PA and the Contractor to send and receive files.

3.1.6 Other Interfaces

1) The Contractor must provide a web-based client interface. This interface will be used by clients to view their balance and transaction history (minimum of 60 days). The website must be available in both English and French versions.

2) For settlement of prepaid card payments, the Contractor must interface with either the Automated Clearing Settlement System (ACSS) or directly with the Bank of Canada. See section 4.1.8 for further information.
3) The Contractor must interface with a bank account specified by the PA to fund the instant issuance prepaid cards.

3.1.7 Protection of Cardholder Data

The protection of customer account information from misuse or fraudulent activity is of utmost concern for the Government of Canada.

For all services provided under this contract, the Contractor and any sub-contractors must employ methods to protect the data according to industry standards and must meet requirements for suppressing/truncating/masking account number and other Cardholder and card information, as specified by Visa, MasterCard, AMEX and as stated in the Payment Card Industry (PCI) Data Security Standards regarding the protection of stored Cardholder data such as data encryption and masking account number when displayed. Equivalent levels of protection must be implemented should the Contractor operate through Interac.

3.1.8 Flexibility

Payment volume and amounts can fluctuate over the course of the year, with large spikes in volumes and amounts occurring regularly (tax refunds, seasonal EI for example). A sharp increase is expected in April 2016 when the use of prepaid cards becomes mandatory for beneficiaries who have not registered in the direct deposit program or qualify as exceptions.

1) The Contractor must be able to handle fluctuating payment levels, both volumes and dollar amounts.
2) There may be times when a large number of beneficiaries are enrolled into the prepaid card program at the same time. The Contractor must be able to handle fluctuating numbers of enrolments.

3.1.9 Additional Contractor Requirements

The Contractor must, on an ongoing basis, work proactively with the PA to determine and propose any improvements or new methodologies for prepaid cards and instant issuance prepaid cards that may improve the RG's services to beneficiaries.

4 Receiver General Requirements – Prepaid Cards

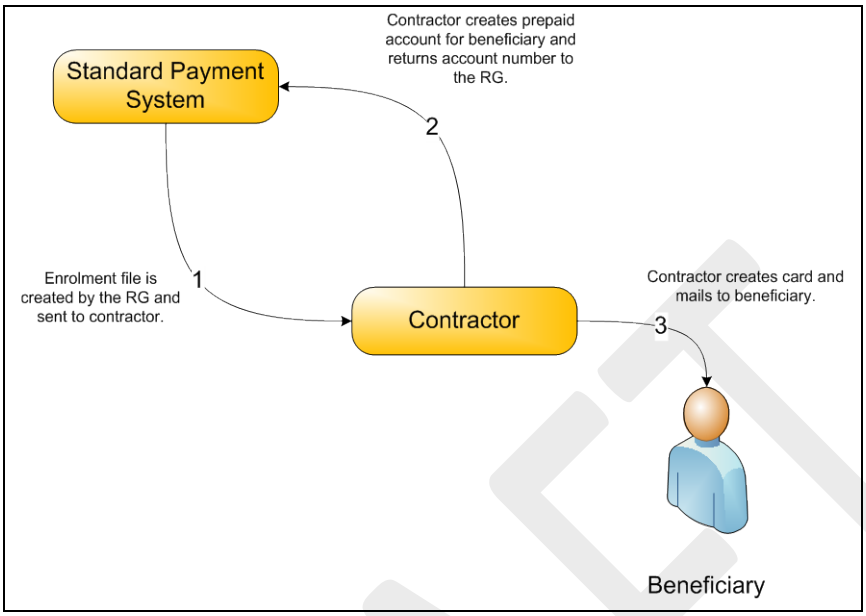
Payments may be initiated by any government department, but payment instructions will be consolidated by the RG and the Contractor will receive payment instructions from a single source.

4.1.1 Card and Account Requirements

1) The Contractor must issue branded MasterCard, Visa, American Express or Interac open loop reloadable prepaid cards to beneficiaries upon notification from the RG.
2) The prepaid card solution being sought by the RG is a banking service and the cards must be a product offered by a bank.
3) The cards must be customized with the Cardholder's full name.
4) The PA must have final approval for the card design and appearance.

5) The cards must comply with the Financial Consumer Agency of Canada (FCAC) regulations on prepaid cards will be going into force on May 1st, 2014. A link to the regulations can be found in section 9.3 of this document.
6) The cards must allow access to funds through ATMs, Point of Sale transactions and access to funds through bank tellers.
7) The cards must allow Cardholders to set up bill payments from their prepaid account.
8) There must be no maximum transaction amount associated to the card, with the exception of maximum daily amounts that may be in place on ATMs.
9) The cards issued by the Contractor must be chip and PIN enabled. The Contractor must provide a method for beneficiaries to change their PIN.
10) The cards must not expire.
11) The Contractor must not allow any overdraft, credit or advances of funds to be associated to this card. Only the balance on the card can be used by the beneficiary.
12) The Contractor must not accept any funds to be loaded onto the prepaid card that do not originate from the RG. This includes preventing the beneficiaries themselves from adding funds to the card.
13) The Contractor must not enforce any minimum or maximum value to the prepaid card account.
14) The Contractor must keep Cardholder information under strict confidence and must not disclose any Cardholder personal or account information for any purpose unless otherwise authorized and required by law. The Contractor must not use any Cardholder personal or accounting information for any marketing or promotion purposes, other than those provided by the PA.
15) The Contractor must adhere to Canada Post mailing standards for any mail sent to beneficiaries as part of the prepaid card program. This includes card mailings, statements and any instructional information that may be required.
16) The card must not be associated with any loyalty or award programs.

4.1.2 Enrolment



Once new beneficiaries are enrolled in the RG's SPS, an enrolment file is sent to the Contractor. The enrolment file will contain beneficiary information including:

- Beneficiary Name
- Beneficiary Address
- Date of birth
- Unique identifier from SPS

Any additional fields that may be required will be determined jointly by the PA and the Contractor.

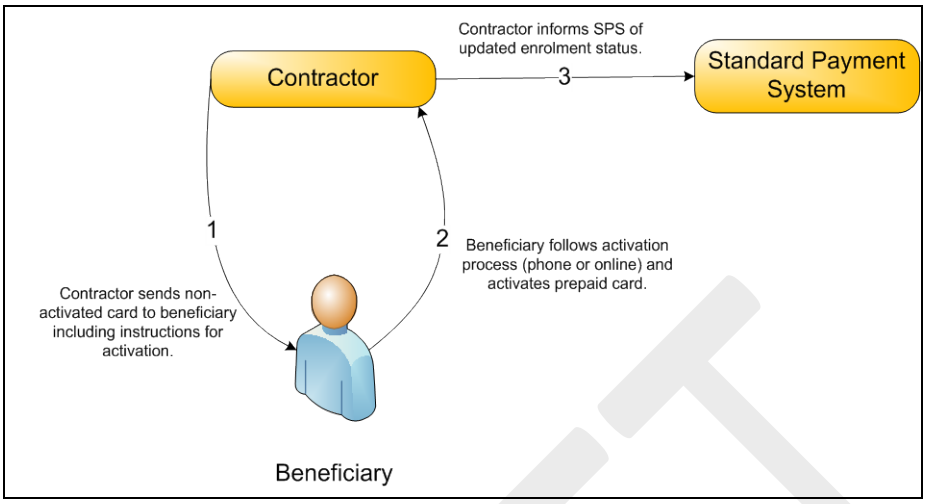
The enrolment file may also contain updated information for existing Cardholders.

1) The Contractor must update their database with the new enrolments and updated information the same day it is received.
2) The RG will have assigned a unique identifier to each beneficiary within the SPS. The Contractor must provide a return file (exact file structure to be determined by the Contractor and the PA) containing an account number for each new beneficiary. This account number indicates where funds will be sent and will be the number used by the PA when requesting the load of funds.

Note that prepaid cards will only be issued to addresses within Canada.

4.1.3 Activation

The exact details of the activation process will be determined jointly by the Contractor and the PA. The requirements in this section are a minimum. Elements that may be required (a challenge question or phone number for example) may be added to the process.

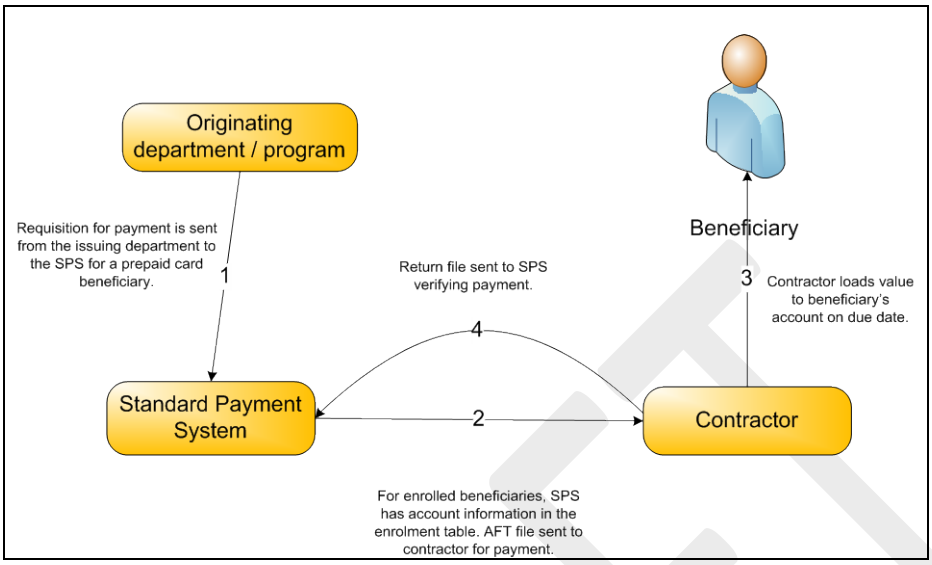


1) The package sent to the beneficiary containing the prepaid card must contain information regarding the activation process.
2) The Contractor must provide interfaces for the Cardholder to activate their card:
    a. Telephone: The Contractor must provide a toll free number and activation process the beneficiary can use to activate their card by telephone. The identification questions/processes to follow will be determined by the Contractor and the PA.
    b. Online: The Contractor must provide a web interface Cardholders may use to activate their cards online.
3) Once activated, the Contractor must inform the RG via file of the change in status of the enrolment.
4) The Contractor must use an activation process that minimizes the risk of fraudulent activation with zero liability to the RG.

4.1.4 Unsuccessful Activation

1) The Contractor must log unsuccessful activation attempts.
2) A weekly report must be provided to the PA detailing the Cardholder names and unsuccessful activations including the times and dates.

4.1.5 Payment Load



An Automated Funds Transfer (AFT) file will be sent to the Contractor each banking day from SPS containing payment instructions including account number, due date, payment program name and payment amount. This file will be sent to the Contractor no later than 3:00 p.m. Payment instructions will be sent with a maximum lead time of 4 banking days. At a minimum, payment instructions will be provided by 3:00 p.m. the day before payment is due.

Payment instructions will be sent by the RG in a CPA standard 005 file.

The payment instructions will be sent in accordance with CPA rule G12 for direct deposits.

1) The Contractor must edit the file upon receipt to determine any payments to be rejected or problems with the file.
2) The Contractor must load value into the designated account by the opening of the business day on which the payment is due..
3) All payments must be issued in Canadian dollars only.

Note that if the Contractor already receives an AFT file from the RG for direct deposits, a separate file will still be used for the Prepaid Card payments.

4.1.6 Unsuccessful Load

In the case of an unsuccessful AFT file load, the Contractor must notify the PA immediately of the failure.

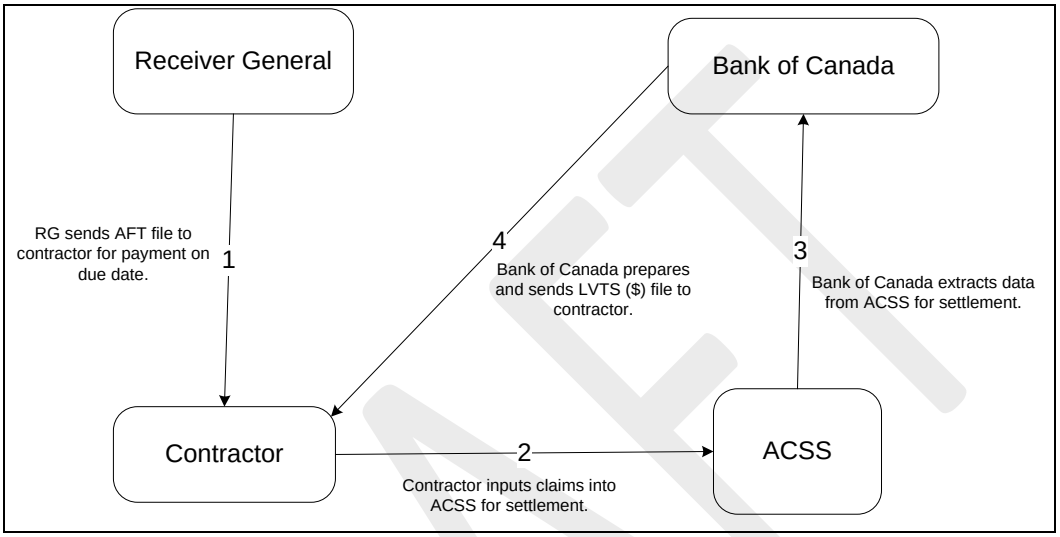
4.1.7 Returned and Rejected Transactions

1) On the business day following the file edit day the Contractor must provide a file containing rejected payments.
2) On the business day following payment due date the Contractor must provide a file containing returned payments. Funds must be returned to the RG within 24 hours.

4.1.8 Settlement

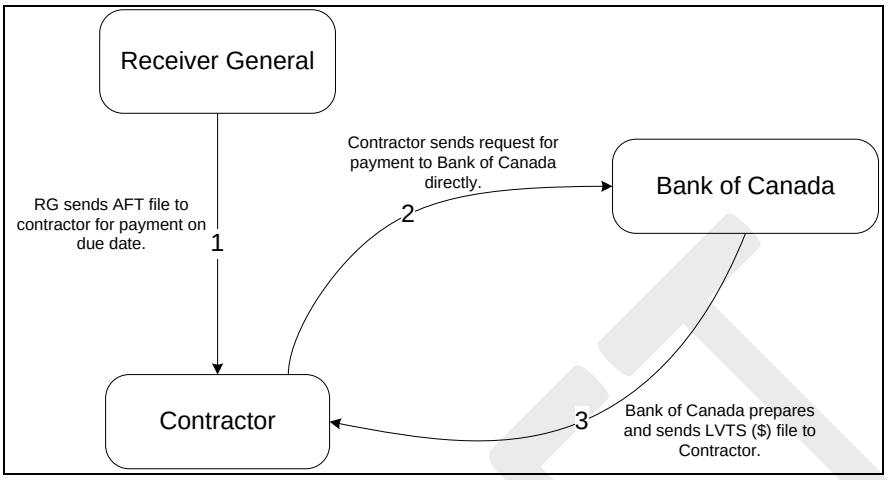
The Contractor may specify if they wish to settle with the RG through the ACSS (if they are already ACSS participants) or by a direct claim to the Bank of Canada. The Contractor must commit to a choice prior to the start of the prepaid card program.

ACSS



1) On the due date, after payment has been made to the beneficiary, the Contractor must enter a claim into the ACSS Stream M for the full amount issued onto prepaid cards that day. This claim must be entered prior to 9:30am Ottawa time.
2) As the prepaid card claim may otherwise be indistinguishable from other direct deposit claims, the Contractor may be required to use a distinct delivery number in their claim to identify the prepaid card claim.
3) The Contractor will receive an LVTS payment from the Bank of Canada to settle the claims from ACSS by 11:00 am the same day.

Direct claim to the BoC



On due date, after payment has been made to the beneficiary, the Contractor must send a claim directly to the Bank of Canada for the full amount issued onto prepaid cards that day. If this claim is entered by 2:30 pm Ottawa time, settlement will be made same day by LVTS payment from the Bank of Canada.

The exact method of claim with the Bank of Canada will be determined by the PA and the Contractor. Options may include the transmission of SWIFT messages, faxes or email claims.

4.1.9 Card Replacement

1) Beneficiaries will contact the service provider if they require a new card to be issued. The Contractor must confirm their identity and mailing details and mail a replacement card.
2) The service provider must cancel the lost card immediately upon being informed by the beneficiary.
3) Upon successful activation of a replacement card, the Contractor must make the full balance of the account available to the beneficiary.

4.1.10 Cardholder Statements

1) The Contractor must provide a web based interface with unlimited monthly access for beneficiaries to view balance and transaction history.
2) The Contractor must provide monthly statements by email to beneficiaries if requested.
3) Statements must include program name information as listed in the payment file. This will allow beneficiaries to determine the source for each payment. The full name of the program (where available) can be found from the Transaction Type code in the CPA standard 005 file.
4) Beneficiaries must be allowed unlimited use of the toll-free support number for balance checks and transaction questions.

4.1.11 Reporting to PWGSC

1) The Contractor must provide a report listing beneficiaries names and account numbers who have not activated their prepaid card eight (8) weeks after issuance.

2) The Contractor must provide a daily file for reconciliation including the number of payments contained on the file, the total dollar amount and the date and time posted.
3) A weekly report providing the number of activated cards.
4) The Contractor must work with the PA to generate ad-hoc reports which may be required of the prepaid card data. The PA will consolidate departmental reporting requests and present them to the Contractor; all requests for reports will come from the PA.

The format of the reports will be determined jointly by the Contractor and the PA.

4.1.12 Recalls

1) Payment recalls will be issued by 12:00 noon Ottawa time on the day before due date. The Contractor must recall the payment on a best effort basis before the transaction has been credited to the beneficiary's account.
2) The Contractor must notify the PA of the disposition of the recall request within four banking days.

4.1.13 Trace Requests

1) The Contractor must perform trace requests as required by the PA, at any time after the date of initial payment.
2) If the trace determines funds were credited to the incorrect account, the Contractor must attempt to recover the amount from the incorrect account on a best effort basis. If the funds cannot be recovered, and the funds were misdirected by the Contractor’s error, the Contractor must reimburse the RG for the full amount misdirected.

4.1.14 Prepaid Card Training

The Contractor must provide training to the PA and requesting programs to enable users to explain the prepaid card program to beneficiaries.

4.1.15 Additional Prepaid Card Requirements

1) Unclaimed balances in a prepaid card account must be transferred to the Bank of Canada after 10 years of inactivity. Notices must be sent to the Cardholder after 2 and 5 years of inactivity.
2) The Contractor must work with the estate of a deceased Cardholder to ensure funds are transferred from the Cardholder’s prepaid card account to their estate.
3) If a payment is erroneously made to a deceased beneficiary, the RG Cheque Redemption Control Directorate (CRCD) will notify the Contractor. The Contractor must return the payment to CRCD when notified.

5 Receiver General Requirements – Instant Issuance Prepaid Cards

In certain circumstances the RG is required to issue payments with little or no advance notice. This is currently done through the use of “priority print” cheques, which are government cheques that can be printed on site and on demand, as opposed to the standard process of having a cheque printed and mailed from a central printing site. As part of the paper cheque phase out, an electronic option is being sought to replace these priority print paper cheques. The RG requires instant issuance prepaid cards that can be stored at the specified locations and loaded with the required amount, activated and provided to the beneficiary immediately as required.

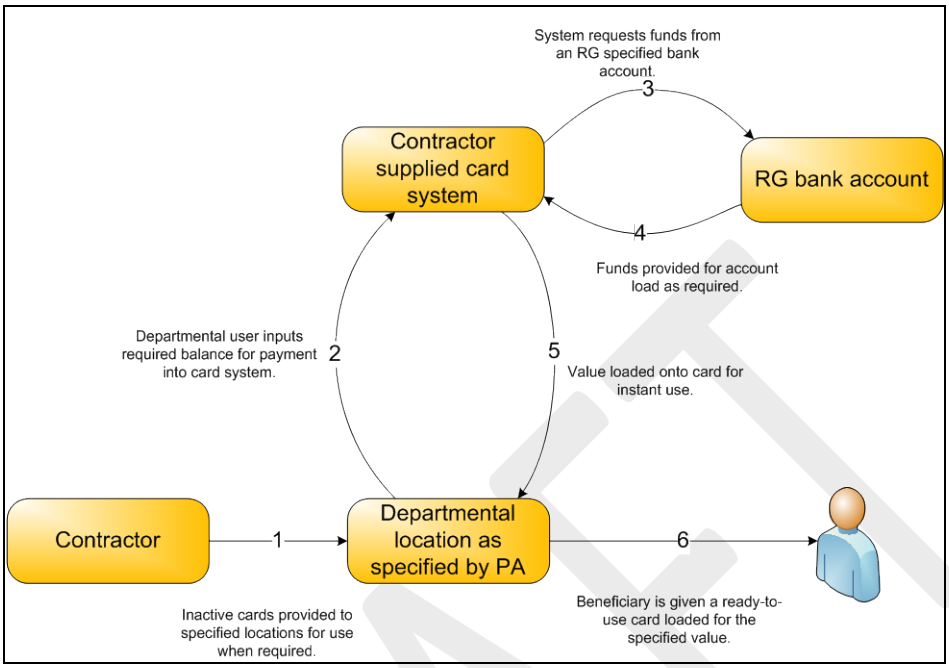
5.1.1 Instant Issuance Prepaid Card Requirements

1) The Contractor must provide MasterCard, Visa, American Express or Interac branded open loop, non-reloadable prepaid cards to departments as specified by the PA. The cards must not be activated and have a zero (0) balance when provided.
2) The PA must have final approval for the card design.
3) The cards must comply with the Financial Consumer Agency of Canada (FCAC) regulations on prepaid cards will be going into force on May 1st, 2014. A link to the regulations can be found in section 9.3 of this document.
4) The cards must allow access to funds through ATMs and bank tellers
5) The cards must allow use at POS devices
6) There must be no maximum transaction amount associated to the card, with the exception of maximum daily amounts that may be in place on ATMs.
7) The cards issued by the Contractor must have chip & PIN technology. The Contractor must provide a method for beneficiaries to choose and change their PIN.
8) The cards must not expire.
9) The Contractor must not allow any overdraft, credit or advances of funds to be associated to this card. Only the balance on the card can be used by the beneficiary.
10) The Contractor must not accept any funds to be loaded onto the prepaid card after the initial load at activation.
11) The Contractor must not enforce any minimum or maximum value to the instant issuance prepaid card.
12) The Contractor must keep Cardholder information under strict confidence and must not: disclose any Cardholder personal or account information for any purpose unless otherwise authorized and required by law; and use any Cardholder personal or accounting information for any marketing or promotion purposes.

5.1.2 Customized Services in Departmental Offices

1) The Contractor must provide non-activated, numbered instant issuance prepaid cards to certain departments. A list of departmental offices requiring these cards will be provided by the PA. See section 9.1 for information regarding estimated numbers required.
2) The Contractor must provide a method for loading value onto the instant issuance card. Funds must be available immediately to the beneficiary upon loading of the card.
3) The Contractor must provide a method for cancelling cards in the event an instant issuance card is reported lost or stolen.

5.1.3 Instant Issuance Card Issuance & Loading



The Contractor provided system must be able to fund the cards from an RG specified zero balance account. The funds must be available for use by the Cardholder without delay. (maximum of 10 minutes)

5.1.4 Instant Issuance Cardholder statements

1) A website must be available for Cardholders to view balance on their card.
2) Beneficiaries must be allowed unlimited use of the toll-free support number for balance checks and transaction questions.

5.1.5 Instant Issuance Training

The Contractor must provide training to the PA and requesting programs in the operation of the instant issuance prepaid card software and process.

5.1.6 Additional Instant Issuance prepaid Card requirements

1) Unclaimed balances on an instant issuance prepaid card must be transferred to the Bank of Canada after 10 years of inactivity. Notices must be sent to the Cardholder after 2 and 5 years of inactivity.
2) The Contractor must work with the estate of a deceased Cardholder to ensure funds are transferred from the Cardholder's instant issuance prepaid card to their estate.

6 General Requirements

Please note that unless otherwise indicated, the following sections apply to both Prepaid Cards and Instant Issuance Prepaid Cards.

6.1 Start Up and Ease of Transition

6.1.1 Start of Prepaid Card program

Due to departments enrolling beneficiaries at different times and respecting different deadlines, beneficiary numbers could increase quickly over short periods. The Contractor must be equipped to adapt to fluctuating enrolment and payment volumes.

6.1.2 Start of Instant Issuance Prepaid Card program

As this is a new payment program being offered to departments, at start up all specified locations will require an initial supply of instant issuance prepaid cards and access to the system to activate and load value.

6.1.3 Transition to a new Contractor

1) The Contractor must ensure a smooth transition from any existing Contractor and to any new Contractor at the end of this contract with no break in service and with minimal disruption to government processes and operations.
2) The prepaid cards and instant issuance prepaid cards issued by the Contractor must remain active and available for Cardholder use even after the contract period has expired and the RG is no longer loading the account. Funds will not be transferred to a new contractor.

6.2 Project Management Requirements

6.2.1 Project Management Approach

The requirement for effective project management will be very demanding during the implementation phase. The Contractor must utilize project management procedures that will ensure the efficient and timely delivery of the required services and outputs.

6.2.2 Contractor-Supplied Resources

1) The Contractor must provide a Project Manager who will act as the point of contact for all matters concerning this contract.
2) The Project Manager must be responsible for overseeing the delivery and implementation of the two card programs, ongoing program support and problem resolution.

6.2.3 PWGSC Supplied Resources

The PA will act as the point of contact for all matters concerning this project.

6.3 Contingency and Disaster Recovery Plan

The Contractor must have a formal Contingency and Disaster Recovery Plan in place, in the event of a power shortage, fire, labour dispute or any other situation that could lead to a disruption in provision of this service, and a copy is to be provided upon request.

6.4 Periodic Threat and Risk Assessments

Upon the PA's request the Contractor must have a Threat and Risk Assessment performed on IT systems and business processes pertinent to the prepaid card services provided.

7 Service Levels

7.1 Service Desk

1) A toll free telephone customer service line must be available 24 hours per day, 365 days per year in both English and French
2) The average on-hold time for the toll-free customer support for beneficiaries to speak with a live representative must be five (5) minutes or less

7.2 Website

7.2.1 Prepaid Cards

1) Excluding scheduled service windows, the web site for beneficiaries must be available 24 hours a day, 365 days a year in both English and French. Minimum monthly availability of 99% is expected (excluding service windows).
2) To ensure the website is accessible to Cardholders who may have disabilities, the site must be compliant with the Web Content Accessibility Guidelines (WCAG) 2.0 technical standard.

7.2.2 Instant Issuance Prepaid Cards

Excluding scheduled service windows, the web service used to activate and load value to the instant issuance prepaid cards must be available 24 hours a day, 365 days a year in both English and French. Minimum monthly availability of 99% is expected (excluding service windows).

7.3 Card Issuance

7.3.1 Prepaid Cards

1) Upon receipt of a new enrolment, the Contractor must mail a card to the beneficiary within 48 hours
2) Replacement cards must be mailed to beneficiaries within 48 of the Contractor being informed of the request.

7.3.2 Instant Issuance Prepaid Cards

1) Non-activated cards must be provided to locations specified by the PA within 7 days of the request.
2) The issuing process must allow funds to be fully available on the cards within 10 minutes of issuance.

8 Fees and Costing

An objective of the prepaid card initiative is to decrease the costs associated with issuing payments from the RG. If the costs associated to operating a prepaid card program exceed the costs associated with the continued use of paper cheques, or the levels of savings do not justify the additional work required to implement the new program, the RG reserves the right not to award the contract.

1) The Contractor must not charge a monthly account fee to the Cardholder.
2) The Contractor must provide the prepaid cards to the recipient at no cost to the Cardholder as well as replacement cards as required.

3) The Contractor must load all payments, with no minimum dollar value requirements, at no cost to the Cardholder.
4) The Contractor must allow unlimited in-network ATM withdrawals and balance inquiries at no cost to Cardholders. A minimum of XXXX ATMs across Canada must be available that are considered in-network to the Cardholder.
5) The Contractor must provide free Website or telephone account balance inquiries.
6) The Contractor may not impose fees on Cardholders for account maintenance and inactivity.
7) The Cardholder must be able to make retail purchases without incurring any fees.
8) The Cardholder must be able to contact the Contractor's customer service representatives via telephone as often as required in order to make inquiries or resolve issues with their accounts.
9) The Contractor must provide the Cardholder with a list of all potential charges/fees as part of the instructional material upon issuance and/or delivery of the prepaid card.
10) Currency conversion fees for international transactions will be charged to the Cardholder.

9 Appendices

9.1 Current and Forecasted Volume Statistics

Exact numbers of cards required, payment volumes and amounts cannot be accurately predicted due to a number of factors, including continued enrolment in direct deposit, the number of the approved exceptions to the card program who will still receive cheques and the unpredictable nature of the beneficiaries. The numbers below represent the forecasted total number of paper cheques that will be issued to individuals for the ten largest programs once the majority of the phase-out is completed and a 95% direct deposit enrolment rate has been achieved, as well as the average payment for each program. The cheque volumes from the programs listed accounts for approximately 90% of the total number of paper cheques issued by the RG. Most importantly, please note that these numbers include an overlap between benefits and recipients. For example most recipients of OAS also receive CPP. Exact numbers are not available to determine the number of unique beneficiaries that would require cards.

Estimates of paper cheque volumes:

Benefit Name	Payment Schedule	Projected Yearly Cheque Volume	Estimated Average Amount per payment	Estimated Annual Dollar Value
CRA T1 Tax Refund	Annual	819,086	$1,754.44	$1,437,037,241.84
GST / HST Credit	Quarterly	1,463,596	$111.87	$163,732,484.52
Universal Child Care Benefit	Monthly	978,491	$137.32	$134,366,384.12
Ontario Child Benefit	Monthly	311,656	$683.97	$213,163,354.32
Canada Child Tax Benefit	Monthly	1,271,359	$225.15	$286,246,478.85
Old Age Security	Monthly	3,095,389	$741.76	$2,296,035,744.64
Canada Pension Plan	Monthly	3,033,325	$536.87	$1,628,501,192.75
Ontario Trillium Benefit (OTB) / Ontario Sales Tax Credit (OSTC)	Monthly	1,534,704	$82.16	$126,091,280.64
BC Low Income Climate Action Tax Credit	Monthly	242,300	$156.75	$37,980,525.00
Employment Insurance	Twice/month	1,153,322	$579.47	$668,315,499.34
Totals		13,903,228		$6,991,470,186.02

Note: This is in no way a guarantee of a level of business but an estimated forecast of the state

of paper cheques once a 95% enrolment rate in direct deposit has been achieved. Also note that beneficiaries enrolled in the prepaid card program may at any time opt to enroll in direct deposit.

Instant issuance prepaid card requirements:

The current estimated number of instant issuance prepaid cards is approximately 6000 cards per year, which may be issued from 32 different locations. However, future requirements of the RG may increase those figures should additional programs determine instant issuance cards would benefit their programs. Currently, the majority of instant issuance prepaid cards will need to be funded with less than $500, but there may be cases where the amounts are substantially higher.

9.2 Acronyms and Definitions

AFT (Automated Funds Transfer) - A system developed and maintained by CPA members to exchange financial data in electronic media.

ACSS (Automated Clearing and Settlement System) – Automated system operated by the CPA to facilitate clearing and settlement for Canadian payment items.

FCAC (Financial Consumer Agency of Canada) – A federal agency established to consolidate and strengthen oversight of consumer protection measures in the federally regulated financial sector, and to expand consumer education.

LVTS (Large Value Transfer System) – A wire payment system maintained by the CPA to facilitate the transfer of large sums of money.

PA (Project Authority) – an individual responsible for the day-to-day management of a contract.

POS (Point of Sale) – The place where a retail transaction is completed.

PWGSC (Public Works and Government Services Canada) – a common services agency for the Government of Canada's departments and agencies. Also the department responsible for RG operations.

RG (Receiver General for Canada) – responsible for making and accepting payments on behalf of the government of Canada, and preparing the Public Accounts of Canada.

SPS (Standard Payment System) – the treasury system used by the RG to issue payments.

9.3 Applicable Documents

The Treasury Board of Canada Secretariat (TBS) policies and publications pertaining to the Official Languages Act pertaining to the applicable service requirements described herein can be viewed by accessing the following web site:

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26160&section=text

TBS policies and publications relating to access to information and privacy, regulations, policies and principles, can be viewed by accessing the following web sites:

http://www.tbs-sct.gc.ca/pol/index-eng.aspx

CPA Standard 005 is the format for the payment files to be used for prepaid cards.

http://www.cdnpay.ca/imis15/pdf/pdfs_rules/standard_005.pdf

CPA rule G12 details the procedures for direct deposits from PWGSC.

http://www.cdnpay.ca/imis15/pdf/pdfs_rules/rule_g12.pdf

FCAS Regulations on Prepaid cards (to go into force May 1, 2014)

http://www.gazette.gc.ca/rp-pr/p2/2013/2013-12-04/html/sor-dors209-eng.php

TECHNICAL CRITERIA

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 the experience of the Bidder will be considered.

Number	Mandatory Technical Criterion	Bid Preparation Instructions
MT1	The Bidder must be: 1. a member of the Canadian Payments Association (CPA), or have an agreement with a CPA member; and 2. a Large Value Transfer System (LVTS) participant, or have an agreement with an LVTS participant.	With its technical bid, the Bidder should submit proof of its CPA membership or its agreement with a CPA member. The Bidder should submit proof that it is an LVTS participant or has an agreement with an LVTS participant.
MT2	The Bidder or the Bidder's subcontractor, if applicable, must have agreements with Visa, MasterCard, American Express (AMEX) or Interac.	With its technical bid, the Bidder should submit proof of such agreement.
MT3	The Bidder providing Visa, MasterCard or Amex prepaid cards must be compliant with Payment Card Industry (PCI) Data Security Standards (DSS).	With its technical bid, the Bidder should submit its attestation of compliancy provided by a card brand or the PCI council, or a Qualified Security Assessor (QSA).
MT4	At bid closing, the Bidder must have acquired experience providing Visa, MasterCard, AMEX, or Interac prepaid card services for 2 years during the last 5 years.	The Bidder should provide: 1. A brief description of the experience(s); 2. Reference information, including the name(s) of the client(s) for which the service was provided, and contact information; and, 3. The starting and finishing date of the services provided to the client(s) (Please note that the Bidder should demonstrate, by providing 1 or more client services, that the Bidder has provided prepaid card services during the past 5 years)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN891-130377/B
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Public Works and Government Services Canada	2. Branch or Directorate / Direction générale ou Direction: Banking Arrangements Direct.
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 prepaid card services to departments as detailed in the attached SOW.

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

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?

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☐ No Non ☑ Yes Oui

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

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No Non ☐ Yes Oui

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

Security and Privacy Requirements

Table of Contents

Acronyms

Acronym	Description
AC	Access Control
AU	Audit & Accountability
CA	Certification and Accreditation
CM	Configuration Management
CP	Contingency Planning
GC	Government of Canada
IA	Identification and Authentication
IT	Information Technology
ITSR	IT Security Requirements
MA	System Maintenance
PE	Physical and Environmental Protection
PGS	Policy on Government Security
PL	Security Planning
PP	Policies & Procedures
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	Security Function Isolation
SI	System and Information Integrity
TBS	Treasury Board Secretariat

Introduction

This Annex describes the minimum security and privacy requirements that the Contractor should meet to ensure that the security and privacy measures specified in this document are implemented and maintained throughout the operation of the Prepaid Card Service requirement. These requirements have been developed based on a combination of Government of Canada (GC) security policies and industry best practices.

Certification and Accreditation

The contracted Prepaid Card Service requirement will be subject to the Government of Canada Certification and Accreditation (C&A), now referred to as the Security Assessment and Authorization (SA&A) process. The service must be fully accredited prior to proceeding to full operations. The “Certifier and Accreditor” will be the office of PWGSC Information Technology Security Directorate, Public Works and Government Services Canada (ITSD/PWGSC).

The C&A process is a rigorous review of all the security functionality of the service designed to ensure that appropriate security controls have been established, their functionality has been tested, verified and validated, specific configuration controls have been established to maintain the system, the operational security risks are known and understood and that the operational security risks do not exceed the target risk level of Medium.

The Contractor must, upon the request from the Contracting Authority complete the Security and Privacy Requirements, Sections 1 and 2 by: (1) indicating (by use of a checkmark next to the corresponding requirement in the validation column) each requirement it satisfies; and (2) providing evidence (e.g. refer to comparable internal/corporate/industry standard/policies) to support each satisfied requirement or a compensating safeguard (e.g. refer to comparable internal/corporate/industry safeguards) to support each unsatisfied requirement.

1. Security and Privacy Requirements for Canadian and Foreign Suppliers

1.1 Policies & Procedures (PP)

Following table lists the requirements related to the PP domain for the CAS.

Table C-1: PP Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
PP-01	POLICY AND PROCEDURES	• The Contractor develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Contractor entities, and compliance for the following at a minimum annually: o Access Control o Security Awareness and Training o Audit and Accountability o Security Assessment and Authorization o Configuration Management o Contigency Planning o Identification & Authentication o Incident Response o System Maintenance o Media Protection o Security Planning o Personnel Security o Risk Assessment o System & Services Acquisition o Security Function Isolation o System & Information Integrity • The Contractor develops, disseminates, and reviews/updates a formal, documented procedures to facilitate the implementation of the policies and associated controls for the following at a minimum annually:		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		o access control. o security awareness and training. o audit and accountability. o security assessment and authorization. o configuration management policy and associated configuration management controls. o contingency planning, including an audit cycle for the contingency plan program as the basis of regular reporting to TBS. o identification and authentication. o 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. o information system maintenance. o media protection. o physical and environmental. o security planning. o personnel security. o risk assessment. o system and services acquisition. o system and communications protection. o system and information integrity. • The Contractor must make its generic security policy and procedures available to the Project Authority upon request.		

1.2 Security Planning (PL)

Following table lists the requirements related to the PL domain for the CAS.

Table C-2: PL Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		•		
PL-04	RULES OF BEHAVIOUR	• The Contractor: o 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; o 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; and o 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.		

1.3 Physical & Environmental Protection (PE)

Following table lists the requirements related to the PE domain for the CAS.

Table C-3: PE Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
PE-09	POWER EQUIPMENT AND POWER CABLING	• The Contractor protects power equipment and power cabling for the information system from damage and destruction.		
PE-10	EMERGENCY SHUTOFF	• The Contractor provides the capability of shutting off power to the information system or individual system components in emergency situations. • The Contractor places emergency shutoff switches or devices in location by information system or system component to facilitate safe and easy access for personnel. • The Contractor protects emergency power shutoff capability from unauthorized activation.		
PE-11	EMERGENCY POWER	• The Contractor 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.		
PE-12	EMERGENCY LIGHTING	• The Contractor 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 Contractor employs and maintains fire suppression and detection devices/systems for the information system		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		that are supported by an independent energy source.		
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	• The Contractor maintains temperature and humidity levels within the facility where the information system resides at acceptable levels.		
PE-14-01	TEMPERATURE AND HUMIDITY CONTROLS	• The Contractor 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 Contractor 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 Contractor 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 Contractor: o employs management, operational, and technical information system security controls at alternate work sites; o assesses the effectiveness of security controls at alternate work sites; and o provides a means for employees to communicate with information security personnel in case of security incidents or problems.		
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	• The Contractor positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.		

1.4 Personnel Security (PS)

Following table lists the requirements related to the PS domain for the CAS.

Table C-4: PS Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
PS-03	PERSONNEL SCREENING	• The Contractor screens individuals prior to authorizing access to the information system in accordance with the *TBS Personnel Security Standard*. • The Contractor rescreens individuals according to conditions requiring rescreening. • For Foreign Contractors, see Section 2 – Security and Privacy Requirements for Foreign Suppliers (Personnel Screening).		
PS-04	PERSONNEL TERMINATION	• The Contractor, upon termination of individual employment, terminates information system access. • The Contractor, upon termination of individual employment, conducts exit interviews. • The Contractor, upon termination of individual employment, retrieves all security-related organizational information system-related property. • The Contractor, upon termination of individual employment retains access to organizational information and information systems in accordance with the TBS Personnel Security Standard.		
PS-06	ACCESS AGREEMENTS	• The Contractor ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		• The Contractor reviews/updates the access agreements when necessary.		
PS-06-01	ACCESS AGREEMENTS	• The Contractor 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; (b) Satisfy associated personnel security criteria; and (c) Have read, understood, and signed a nondisclosure agreement.		
PS-07	THIRD-PARTY PERSONNEL SECURITY	• The Contractor establishes personnel security control requirements including security roles and responsibilities for third-party providers. • The Contractor documents personnel security control requirements. • The Contractor monitors provider compliance. • The Contractor ensures security screening of private sector organizations and individuals who have access to Protected information and assets. • The Contractor 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 Contractor employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		

1.5 Audit & Accountability (AU)

Following table lists the requirements related to the AU domain for the CAS.

Table C-5: AU Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
AU-07	AUDIT REDUCTION AND REPORT GENERATION	• The Contractor ensures that the information system provides an audit reduction and report generation capability.		
AU-07-01	AUDIT REDUCTION AND REPORT GENERATION	• The Contractor ensures that the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		

1.6 Contingency Planning (CP)

Following table lists the requirements related to the CP domain for the CAS.

Table C-8: CP Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
CP-06	ALTERNATE STORAGE SITE	• The Contractor establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. • The Contractor 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 Contractor establishes an alternate processing site including necessary agreements to permit the resumption		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		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 Contractor 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 Contractor ensures that the alternate processing site provides information security measures equivalent to that of the primary site.		
CP-08	TELECOMMUNICATIONS SERVICES	• The Contractor 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 Contractor: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the Contractor '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 Contractor obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		• The Contractor obtains alternate telecommunications Contractors that are separated from primary Contractors so as not to be susceptible to the same hazards.		
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	• The Contractor 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 Contractor ensures that the information system implements transaction recovery for systems that are transaction-based. • The Contractor 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. • The Contractor protects backup and restoration hardware, firmware, and software.		

1.7 Identification & Authentication (IA)

Following table lists the requirements related to the IA domain for the CAS.

Table C-5: IA Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
IA-03	DEVICE IDENTIFICATION AND AUTHENTICATION	• The Contractor ensures that the information system uniquely identifies and authenticates all devices before establishing a connection.		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
IA-03-01	DEVICE IDENTIFICATION AND AUTHENTICATION	• The Contractor ensures that the information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. • The Contractor 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-06	AUTHENTICATOR FEEDBACK	• The Contractor ensures that the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
IA-08	IDENTIFICATION AND AUTHENTICATION (NON-CONTRACTOR USERS)	• The Contractor ensures that the information system uniquely identifies and authenticates non-Contractor users (or processes acting on behalf of non-Contractor users).		

Table C-6: RA Requirements List

1.8 System & Services Acquisition (SA)

Following table lists the requirements related to the SA domain for the CAS.

Table C-11: SA Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
SA-02	ALLOCATION OF RESOURCES	• The Contractor includes a determination of information security control requirements for the information system in mission/business process planning.		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		• The Contractor determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process. • The Contractor establishes a discrete line item for information security in Contractor programming and budgeting documentation.		
SA-04	ACQUISITIONS	• The Contractor 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 Contractor 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 Contractor includes the development and 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 Contractor requires in acquisition documents that vendors/Contractors 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 Contractor requires in acquisition documents, that		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		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 Contractor obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: o Secure configuration, installation, and operation of the information system; o Effective use and maintenance of security features/functions; o Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. o User-accessible security features/functions and how to effectively use those security features/functions; o Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and o User responsibilities in maintaining the security of the information and information system.		
SA-06	SOFTWARE USAGE RESTRICTIONS	• The Contractor uses software and associated documentation in accordance with contract agreements and copyright laws.		

1.9 Security Function Isolation (SC)

Following table lists the requirements related to the SC domain for the CAS.

Table C-12: SC Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
SC-05	DENIAL OF SERVICE PROTECTION	• The Contractor ensures that 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 Contractor ensures that the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		
SC-08	TRANSMISSION INTEGRITY	• The Contractor ensures that the information system protects the integrity of transmitted information in accordance with section 6.1 of Technical Supply Chain Guidelines (TSCG)-01: Contracting Clauses For Telecommunications Equipment and Services.		
SC-08-01	TRANSMISSION INTEGRITY	• The Contractor employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.		
SC-14	PUBLIC ACCESS PROTECTIONS	• The Contractor ensures that the information system protects the integrity and availability of publicly available information and applications.		
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	• The Contractor issues public key certificates under a certificate policy or obtains public key certificates under an appropriate certificate policy from an approved Contractor.		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
SC-18	MOBILE CODE	• The Contractor: (a) defines acceptable and unacceptable mobile code and mobile code technologies; (b) establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and (c) authorizes, monitors, and controls the use of mobile code within the information system.		
SC-18-01	MOBILE CODE	• The Contractor ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets defined mobile code requirements. • The Contractor ensures that the information system implements: o detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary; o prevents the download and execution of prohibited mobile code; and o prevents the automatic execution of mobile code in software applications and requires defined actions prior to executing the code.		
SC-23	SESSION AUTHENTICITY	• The Contractor ensures that the information system provides mechanisms to protect the authenticity of communications sessions.		
SC-23-01	SESSION AUTHENTICITY	• The Contractor ensures that the information system: o invalidates session identifiers upon user logout or other session termination; o provides a readily observable logout capability whenever authentication is used to gain access to web pages;		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		o generates a unique session identifier for each session and recognizes only session identifiers that are system-generated; and o generates unique session identifiers randomly.		
SC-28	PROTECTION OF INFORMATION AT REST	• The Contractor ensures that the information system protects the confidentiality and integrity of information at rest.		

1.10 Access Control (AC)

Following table lists the requirements related to the AC domain for the CAS.

Table C-7: AC Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
AC-09	PREVIOUS LOGON (ACCESS) NOTIFICATION	• The Contractor ensures that 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 Contractor ensures that the information system notifies the user o upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access; o number of unsuccessful logon/access attempts during a system configurable time period; and o security-related changes to the user's account during a system configurable time period.		
AC-14	PERMITTED ACTIONS WITHOUT	• The Contractor permits specific user actions to be performed without identification and authentication only to		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
	IDENTIFICATION OR AUTHENTICATION	the extent necessary to accomplish mission/business objectives. • The Contractor documents and provides supporting rationale in the operations security plan for the information system, user actions not requiring identification and authentication.		
AC-16	SECURITY ATTRIBUTES	• The Contractor ensures that 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 Contractor ensures that the information system allows authorized entities to change security attributes. • The Contractor ensures that the information system allows authorized users to associate security attributes with information. • The Contractor ensures that 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-20-01	USE OF EXTERNAL INFORMATION SYSTEMS	• The Contractor 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 Contractor: (a) Can verify the implementation of required security controls on the external system as specified in the Contractor's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the Contractor entity hosting		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		the external information system. • The Contractor 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 Contractor: o facilitates information sharing by enabling authorized system operators and priviledged users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances; and o employs organization-defined information sharing circumstances and mechanisms or manual processes required to assist system operators and priviledged users in making information sharing/collaboration decisions.		
AC-21-01	USER-BASED COLLABORATION AND INFORMATION SHARING	• The Contractor ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.		
AC-22	PUBLICLY ACCESSIBLE CONTENT	• The Contractor: o designates individuals authorized to post information onto a Contractor information system that is publicly accessible; o trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information; o reviews the proposed content of publicly accessible information for confidentially sensitive information prior to posting onto the Contractor's information system; o reviews the content on the publicly accessible		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		o Contractor information system for confidentially sensitive information at a minimum annually; and removes confidentially sensitive information from the publicly accessible Contractor information system, if discovered.		

1.11 System Maintenance (MA)

Following table lists the requirements related to the MA domain for the CAS.

Table C-14: MA Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
MA-03	MAINTENANCE TOOLS	• The Contractor approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.		
MA-03-01	MAINTENANCE TOOLS	• The Contractor checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.		
MA-06	TIMELY MAINTENANCE	• The Contractor 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.		

1.12 System & Information Integrity (SI)

Following table lists the requirements related to the SI domain for the CAS.

Table C-15: SI Requirements List

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
SI -08	SPAM PROTECTION	• The Contractor: o 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; and o updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with Contractor configuration management policy and procedures.		
SI-08-01	SPAM PROTECTION	• The Contractor centrally manages spam protection mechanisms. • The Contractor ensures that the information system automatically updates spam protection mechanisms (including signature definitions).		
SI-09	INFORMATION INPUT RESTRICTIONS	• The Contractor restricts the capability to input information to the information system to authorized personnel.		
SI-10	INFORMATION INPUT VALIDATION	• The Contractor ensures that the information system checks the validity of information inputs.		
SI-11	ERROR HANDLING	• The Contractor ensures that the information system: o identifies potentially security-relevant error conditions;		

ID	Requirement Title	Description	Validation	Supporting Evidence / Compensating Safeguard
		o 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; and o reveals error messages only to authorized personnel.		