Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Alain Papineau
Email: alain.papineau@pwgsc.gc.ca
Phone: 613-858-8997

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Cheque Image Exchange Services	
Solicitation No. - N° de l'invitation EN891-193251/A	**Date** 2019-07-31
Client Reference No. - N° de référence du client 20193251	**GETS Ref. No. - N° de réf. de SEAG** PW-$$ZG-404-36705
File No. - N° de dossier 404zg.EN891-193251	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2019-09-09**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Papineau, Alain	**Buyer Id - Id de l'acheteur** 404zg
Telephone No. - N° de téléphone (613) 858-8997 ( )	**FAX No. - N° de FAX** ( ) -
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

THE ONE ON ONE WILL BE TAKING PLACE BETWEEN AUGUST 26TH AND AUGUST 30TH, 2019.

WE WILL REQUIRE YOUR FEEDBACK TO OUR QUESTIONS AND STATEMENT OF WORK BY AUGUST 30, 2019.

REQUEST FOR INFORMATION (RFI) REGARDING THE RECEIVER GENERAL CHEQUE IMAGE EXCHANGE SERVICE FOR PUBLIC SERVICES AND PROCUREMENT CANADA

NATURE OF REQUEST FOR INFORMATION

This RFI is neither a call for tender nor a bid solicitation. No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way a commitment by the Government of Canada, nor as authority to potential respondents to undertake any work that could be charged to Canada. This RFI is not to be considered as a commitment to issue a subsequent solicitation or award contract(s) for the work described herein.

Although the information collected may be provided as commercial-in-confidence (and, if identified as such, will be treated accordingly by Canada), Canada may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third party or personal information. Please note that Canada may be obligated by law (e.g. in response to a request under the Access of Information and Privacy Act) to disclose proprietary or commercially-sensitive information concerning a respondent (for more information: http://laws-lois.justice.gc.ca/eng/acts/a-1/).

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

Respondents will not be reimbursed for any cost incurred by participating in this RFI.

The RFI closing date published herein is not the deadline for comments or input. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

The Crown retains the right to negotiate with suppliers on any procurement.

Documents may be submitted in either official language of Canada.

BACKGROUND OF THIS REQUEST FOR INFORMATION

The Canadian payment industry is moving away from exchanging paper cheques and replacing the paper items with cheque images. The GC, specifically the Receiver General for Canada (RG), is conducting research and collecting information in order that the Receiver General can develop a strategy to align with this cheque image exchange initiative.

The RG expects to leverage the research, experience and development efforts that already exist for cheque imaging within Canada. In the event of a contract, the Contractor would be required to provide

all necessary infrastructure and resources to complete the work**.** The GC, therefore will not consider paying costs required for the development of new systems and will not pay for any development other than that required to provide the required interface(s) between the GC and the Contractor's systems.

The attached draft Statement of Work (SOW) may be included in a future Request for Proposal (RFP). Should an RFP be published and a contract awarded, PSPC anticipates that the services would be required for a period of five (5) years commencing from the date of contract award with an irrevocable option on the part of Canada to extend the period of any resulting contract by up to two (2) additional one (1) year periods, and one (1) additional one (1) year transition period at the end of the option periods.

Public Services and Procurement Canada (PSPC)'s Acquisitions Program implemented a policy on the Phased Bid Compliance Process (PBCP) on July 17, 2017. This policy is available on the BuyandSell website (https://buyandsell.gc.ca/policy-and-guidelines/policy-notifications/PN-123). In the event of a competitive solicitation, the PBCP would provide bidders with an opportunity, after the solicitation closing date and time, to correct a finding of non-compliance with respect to Eligible Mandatory Requirements.

PURPOSE OF THIS REQUEST FOR INFORMATION

The intent of this Request for Information (RFI) is to solicit feedback and industry perspectives. In particular, the PSPC hopes to obtain the following:

a) clarity on the interest level and availability of service providers;
b) industry feedback on the proposed Statement of Work (SOW);
c) ensure potential bidders are aware of the security, privacy and other clauses that will be required within any resulting Contract;
d) encourage potential bidders to participate in discussions with the RG to discuss the proposed SOW.

CONTENTS OF THIS RFI

a) This RFI is a follow-up to the '*RG Cheque Imaging Exchange*' RFI published on February 2nd, 2018 (Solicitation Number EN893-182181/A). This RFI contains an updated Statement of Work found in Annex A. This document remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the document are welcome.

b) This RFI also contains specific questions addressed to the industry. Respondents are requested to refer to and complete Annex B - Questions and Information Requests.

c) Volumetric Data - The data included in this RFI is being provided to respondents purely for information purposes. Although it represents the best information currently available to PSPC, Canada does not guarantee that the data is complete or free from error.

NATURE OF RESPONSES REQUESTED

Respondents are at their own discretion in this regard, but Canada is seeking relevant information, simply and directly stated, in order to avoid undue work by respondents and undue effort by Canada to analyze the results.

Responses from potential suppliers to this RFI will assist Canada in formulating any possible procurement strategy to meet Canada's business and operational requirements.

Respondents are requested to provide comments, concerns, and suggestions, and where applicable, recommendations regarding how the requirements or objectives described in this RFI could be satisfied or improved upon.

Respondents are requested to provide feedback related to the clarity of the draft SOW and pricing information by completing the Annex B - Questions and Information Requests.

With regards to the information requested in Annex B, only written response will be accepted. Respondents should explain any assumptions made when preparing their responses.

FORMAT OF RESPONSES

Cover Page: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the RFI number, the volume number and the full legal name of the respondent.

Title Page: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

* the title of the respondent's response;
* the name, address, email and telephone number of the respondent;
* the date; and
* the RFI number.

ENQUIRIES

Because this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all potential suppliers. However, respondents with questions regarding this RFI may direct their enquiries to:

Contracting Authority: Alain Papineau
E-mail Addresses: Alain.Papineau@tpsgc-pwgsc.gc.ca
Telephone: (613) 858-8997

OPPORTUNITIES FOR DISCUSSON

During the period of this RFI, there will be an opportunity for Canada and Industry to enter into discussions about the requirement during scheduled one-on-one meetings to be held at 11 Laurier Street, Gatineau, Quebec.

The scope of the requirement outlined in the RFI would be reviewed during the meeting and questions would be answered. A discussion can be requested even though a written response to the RFI was not submitted.

Respondents may use this session to better understand the requirements and to explain their comments in regards to the documents attached to this RFI. Meetings will be up to three (3) hours in duration and may be attended in person or by teleconference. Any meeting request must be submitted in writing to the Contracting Authority, noted herein, no later than fifteen (15) business days prior to the closing of the RFI, and must include the names of the representatives who will attend, along with their Title/Responsibility within the company, and at least three proposed (3) time slots (morning or afternoon), and dates, in which they would be available to meet.

Meeting requests received after that time may not be accommodated and PSPC cannot guarantee that any respondent will be allocated any of its preferred meeting times. Respondents who do not request a meeting will not be precluded from submitting a bid, should an RFP be issued in the future.

TREATMENT OF RESPONSES

A) Use of Responses:

Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify procurement strategies or any draft documents contained in this RFI. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.

B) Confidentiality:

Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the Access to Information Act.

C) Follow-up Activity:

Canada may, in its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response. Canada reserves the right to invite any or all respondents to present their submissions to this RFI and/or perform a product demonstration.

•

INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

As part of a future Request for Proposal (RFP), included in their bid, the Bidder will be required to demonstrate compliance with specific Government of Canada IT security requirements. The table below provides possible criteria to which the Bidder must provide responses.

In the event that a contract is awarded, the Contractor will be requested to demonstrate compliance with specific IT security controls. Refer to Annex C – IT Security Controls Profile.

IT Security Area	Bid Submission Requirements
Data Residency and Personnel	The Bidder must clearly demonstrate its data residency compliance and provide a data centre deployment plan(s) which should include specifics on: • location(s) (country and city) of primary data centre(s); • location(s) (country and city) of secondary data centre(s) and backup centres; • location(s) (country and city) of all the infrastructure components (including, but not limited to, database servers, network data storage, application servers); and • location(s) (country and city) of the Security Operations Centre, Network Operations Centre and the Service Desk. The Bidder should clearly demonstrate its business entities and personnel location and provide: • location(s) (country and city) of all business entities performing work under the contract; and

	• location(s) of all personnel performing the work under the contract.
Secure Connection	The Bidder must implement safeguards to ensure that all websites and web services, accessible by the Government and used for the work under this contract, are configured to provide service only through a secure connection, in accordance with Section 6.2.4 of the Policy on the Management of Information Technology and the Policy on Government Security. The Bidder will implement a secure web connection that: • is configured for HTTPS • has HSTS enabled • implements TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, as outlined in the Communications Security Establishment's (CSE): o ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites o ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information • disables known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062 • disables known-weak ciphers (e.g. RC4 and 3DES)
IT Security Policies and Procedures (Controls)	The Bidder should demonstrate its ability to comply with the IT security requirements by maintaining policies and procedures that support IT security throughout the contract by providing evidence of any existing policies and procedures that support the security control families described in ITSG-33. (https://cyber.gc.ca/en/guidance/overview-itsg-33). The Bidder should describe how its policies and procedures align to the security control families by providing the following information on current policies and procedures: • name of policy and/or procedure • its purpose • its scope • the roles and responsibilities that are described within the policy and/or procedure • how it ensures coordination among organizational entities • how it ensures compliance within the organization
IT Security Topology Diagram	The Bidder should provide an IT security topology diagram which should include the following components: • interfaces • web • applications • databases • security devices

	• system management • backup infrastructure The Bidder should provide one or more of the following, which define information systems components and functions to be separated by boundary protection devices: • information system design documentation • information system architecture
Security Organization	The Bidder should describe the experience of the security organization that will be responsible in ensuring the security of, including the name of each person, their role & description of their duties, their experience, and certifications.
Data Segregation	The Bidder should provide its proposed approach to data segregation, that should include: • information system design documentation; • information system architecture; and • process and procedures to support data segregation.
Disposal and Sanitization	The Bidder should provide its proposed approach to the disposal and sanitization of Canada's data, including: • a plan for hard-drive sanitation or an action plan if the system is hosted in a virtual environment that will ensure Canada's data is not obtainable; • a plan for data disposal; • system disposal processes and procedures; • a plan for destruction of duplicate records that may be stored in a records management system or backups; and • the process it plans to follow when the system is no longer required and is being decommissioned.
Continuous Monitoring Service	The Bidder should provide its proposed approach to continuous monitoring and include the following components: • the strategy for continuous monitoring; • established measures, metrics, and status monitoring and control assessments frequencies; • details of data collection and its reporting aspects; • analysis methods of the data gathered and report findings accompanied by recommendations; • response mechanisms to assessment findings to include making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority; and • review and update cycles to support continuous improvement and maturing measurement capabilities.

Industry IT Security Certification	The Bidder should provide proof of its security certification(s) and applicable audit standards for its proposed solution in the form of a copy of a valid certificate or audit standard and describe how the certification or audit standard was assessed and obtained (e.g.: 3rd party, self-assessment) for each IT Security certification and audit standard held, such as: • FedRAMP; • Cloud Security Alliance – STAR; • COBIT; • ISO 27001; • PCI DSS; • CMM; and • any others. The Bidder should also stipulate if the certification or audit standard applies to the whole solution or to a specified portion of their solution.
Identity, Credential and Access Management	The Bidder should provide details on its proposed solution's Identity, Credential and Access Management level of assurance capabilities with respect to TBS Standard on Identity and Credential Assurance. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776). The Bidder should identify the level of assurance and demonstrate how it meets the requirements of that level.

RESULTING CONTRACT CLAUSES

The following clauses and conditions can be expected to apply to and form part of any Contract resulting from a future Request for Proposal (RFP).

A) Statement of Work

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

B) Standard Clauses and Conditions

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

C) General Conditions

SACC Manual Clause: 2035 (2018-06-21), General Conditions – Higher Complexity – Services, would apply and would form part of the Contract.

D) Privacy Clauses

SACC Manual Clause: 4008 (2008-12-12), personal Information, would apply and form part of the Contract.

SACC Manual Clause: A9122C (2008-05-12), Protection and Security of Data Stored in Database, would apply and form part of the Contract.

E) Industrial Security Requirements

The following security related clauses provided by the Contract Security Program (http://www.tpsgc-pwgsc.gc.ca/escsrc/introduction-eng.html) would apply and form part of the Contract:

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 (CISD), Public Works and Government Services Canada (PWGSC).

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 CISD/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, including 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 Industrial Security Manual (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-eng.html).

6. Where safeguarding measures are required in the performance of the work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individual's sites or premises.

7. The Company Security Officer (CSO) must ensure through the Contract Security Program that the Contractor and proposed individuals hold a valid security clearance at the required level.

8. For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

F) Canadian Content Certification

SACC Manual Clause: A3060C (2008-05-12) Canadian Content Certification, would apply and form part of the Contract.

SACC Manual Clause: A3050T (2014-11-27) Canadian Content Definition, would apply and form part of the Contract.

G) Financial Capability

SACC Manual Clause: A9033T (2012-07-16) Financial Capability**,** would apply and form part of the Contract.

H) Legal Evidence

On occasion the Receiver General may need to provide evidence in legal proceedings. To ensure the admissibility and weight of electronic records as documentary evidence, the Contractor must ensure that any cheque images in their custody can be proven or presumed to be reliable, accurate, and authentic. To ensure the trustworthiness of their electronic records, the Contractor should conform to a standard such as the Canadian General Standards Board *'Electronic records as documentary evidence'* (CGSB-72.34-2017). The *Canada Evidence Act* encourages the use of standards for the purpose of determining whether an electronic document is admissible under any rule of law.

ANNEX A

STATEMENT OF WORK

A.1 Purpose

This Statement of Work (SOW) describes the process, and associated requirements, for a Receiver General cheque image exchange solution. The SOW has been prepared with the intention of procuring the proposed solution as a service.

A.2 RG Cheques

The Receiver General (RG) issues a significant number of cheques on behalf of the Government of Canada (GC). RG cheques are also known as '*warrants'*. In fiscal year 2018/2019, the RG issued over 31 million cheques. These cheques are issued under various departmental programs such as child tax benefits, tax refunds, senior's benefits and many others.

The RG does not issue the government cheques through a financial institution, the cheques are drawn on the Bank of Canada. The RG exchanges and clears their cheques directly with the Canadian financial institutions. Since the RG participates in the settlement and clearing with the Canadian direct clearers, the RG respects the rules and standards published by Payments Canada.

The RG is somewhat unique in the cheque clearing process in that the RG only issues cheques, the RG does not cash cheques drawn on the other financial institutions. While the RG does receive cheques as a payee (income tax payments, for example), these cheques are processed under an existing financial services contract and are out of scope for this SOW.

All RG cheques have a unique Cheque Form Number (CFN). The CFN is either 12 digits or 13 digits in length depending on the process and cheque stock used when printing the cheque. The RG cheque number does not include a check digit. Below are images of RG cheques that show these Cheque Form Numbers. The CFN appears on the top right corner of the cheque face as well as within the MICR line. Within the MICR line, the CFN follows the Transit Number which is always '*00000'*, and the Financial Institution which is always '*117'*.

The cheque sample above shows the 12 digit CFN format.

The cheque sample above shows the 13 digit CFN format.

A.3 Cheque Imaging Project

In 2010, Payments Canada (*then known as the CPA - Canadian Payments Association)* initiated the Image Rule Project. This project was a phased initiative which focused on creating efficiencies in the cheque clearing and exchange process for paper payment items and returns through the use of image technology. Paper payment items include cheques, bonds and warrants (RG cheques). The goals of the image project were to reduce complexity in the exchange and clearing of paper payment items by reducing or eliminating the need to move physical paper items between financial institution processing sites. Physical transportation of paper cheques around Canada creates inefficiencies. In addition, the reliance on air and ground transportation to ship cheques means that a portion of Canada's payment system is vulnerable to interruptions for reasons ranging from bad weather to airport security incidents.

The main deliverable of the Image Rule Project was the documented framework, rules and standards to allow financial institutions to exchange files with images of cheques electronically with other financial institutions. However, this shift to an image based processing of cheques will not only improve efficiency and lower costs; it has also allowed financial institutions to introduce new functionalities that provide faster and more convenient customer services. For example, access to cheque images for customers rather than the previous practice of enclosing cancelled cheques with printed customer statements, or allowing a customer to deposit a cheque using their smartphone or tablet.

There are 3 methods for exchanging imaged items:

- a '*Clearing Replacement Document*' (CRD) – a printout of the cheque image including the MICR coding, also referred to as *'forward items'*

- a '*Return Replacement Document*' (RRD) – a printed image of the cheque including the return information and the MICR coding, also referred to as *'returned items'*

- an *'Image Captured Payment'* (ICP) File – a cheque image file that includes a digital image of the front and back of the cheque and the MICR line coding, which can be used for both forward items and returned items

Similar to the RG's experience, financial institutions are still processing significant volumes of paper cheques despite the decline in overall cheque usage. It is the RG's understanding that the majority of financial institutions have made some progress on a cheque imaging solution but are at varying stages of implementation. The financial institutions have begun to image a significant volume of cheques at source, this includes via ATMs, at the branch and via mobile devices (smartphones, tablets, etc.). However,

because most financial institutions are not yet fully capable of creating and/or receiving cheque image files, a large volume of items are still cleared as paper. In these situations the captured images are printed and exchanged as CRDs.

A.4 RG Treasury Systems Renewal

The Receiver General manages and operates a central suite of treasury related applications on behalf of the Government. These applications handle a variety of essential processes that include payment issuance, revenue collection, reconciliation, settlement and reporting. The RG is currently planning a modernization strategy for some of these core applications. This modernization effort will likely take several years to implement. The proposed solution that is described in the SOW has been prepared in an attempt to minimize any modifications or upgrades to the current suite of RG applications.

A.5 Current Situation

The vast majority of RG cheques are printed, enveloped and prepared for mail distribution at two PSPC production centres; one in Quebec City and one in Winnipeg. A small percentage of RG cheques are printed in departmental print sites across Canada.

The cheque recipients cash the RG cheques at a branch of the financial institution of their choice. Methods of deposit vary and include over the counter, via an ATM, via a smart phone, etc. At the end of the business day, the paper cheques collected by each branch are bundled, totaled and bagged, then couriered to the regional processing centre for that financial institution in one of six cities across Canada. The six cities are Halifax, Montreal, Toronto, Winnipeg, Calgary and Vancouver. The RG cheques that have been imaged during the deposit process must be printed as CRDs since the RG does not currently accept cheque image files.

All the paper items, cheques and CRDs, are transported to the RG's cheque processing centre, the Cheque Redemption Control Directorate (CRCD), which is located in Matane, Quebec. Each direct clearer enters a redemption claim against the Government for the value and volume of the cheques said to be contained in the bags of paper items. This redemption claim is entered into a Payments Canada application called the Automated Clearing and Settlement System (ACSS).

CRCD staff manually prepare the cheques and CRDs into trays to be loaded and scanned by the cheque readers. The number of CRCD staff engaged in this activity varies as RG cheque volumes fluctuates during the month with peaks usually a few days after high volume Government program payment dates (e.g. Child Tax Benefit). The scanning of the cheques serves two purposes – the paper item is imaged and a data file is created. This data file carries the cheque form number and the redeemed amount. This data file is input to the RG's cheque redemption and reconciliation application for item reconciliation. The item is verified to ensure that it was issued by the RG, has not been previously cashed and the amount recorded by the financial institution where the cheque was cashed agrees with the issued amount. CRCD staff are alerted to any exceptions or discrepancies.

CRCD staff analyze the exceptions and reconciliation issues, and assist in fraud investigations. CRCD staff also manually prepare any returned items or adjustments which are sent to the Bank of Canada (BoC) for redistribution to the financial institutions. CRCD staff reconciles the volume and value of the items processed with the redemption claims submitted by the financial institutions.

A.6 Cheque Image Files

A cheque image file (*'Image Captured Payment'* (ICP) File) must adhere to the current Payments Canada file layout standard which is the ANSI X9.100-187-2008 file layout (refer to Payments Canada Standard 015: https://www.payments.ca/sites/default/files/standard_015.updated.pdf). Within the SOW, this file layout will be referred to as an '*ICP file'*.

Under the RG's proposed solution as described in this SOW, the RG's treasury applications will not be required to directly process an ICP file.

The data from the ICP files that is essential to the RG is:

- a quality, usable, retrievable image that can be considered as the official and legal representation of the original cheque
- the data needed to confirm that a valid issued cheque has been redeemed only once for the correct amount

The following sections further explain how this data is to be provided by the Contractor to the RG.

A.7 Cheque Image Detail Requirements

This section describes the detailed requirements of the RG cheque image exchange solution which must be delivered by the Contractor.

A.7.1 Objective

The objective of the RG's cheque image exchange solution is for the Contractor to:

- handle the processing of all RG bound ICP files
- provide one standardized data input stream to the RG
- maintain an image archive for all RG imaged items

A.7.2 Rules and Standards

The rules and standards for cheque imaging within Canada are administered by Payments Canada.

The Contractor must ensure that all Payment Canada rules and standards that are applicable to the Government of Canada are respected. This includes, at a minimum, the following rules and standards:

- Rule A4 - Returned and Redirected Items
- Rule A10 - Image Rule
- Rule G3 - Rules Pertaining to the Redemption and Settlement of Government of Canada Paper Instruments
- Standard 013 - Return Replacement Document Design Standard
- Standard 014 - Clearing Replacement Document Design Standard
- Standard 015 - Companion Document to the ANSI X9.100-187-2008 "Specifications for Electronic Exchange of Check and Image Data - Domestic"
- Standard 018 - Payment Item Information Security Standard

The complete set of Payment Canada rules and standards can be found at the following web address:
http://www.payments.ca/about-us/our-systems-and-rules/retail-system/rules-and-standards

A.7.3 Mandatory Elements

The Contractor must provide a cheque image exchange solution that includes the following elements:

- a process to accept incoming ICP files
- a process to transmit redeemed item data to the RG

- an image archive
- a facility for Government employees to have real time access to search, view, and print images
- a business continuity and disaster recovery plan
- all required security and privacy controls

A.7.4 Direct Clearer Bilateral Agreements

The RG will also enter into bilateral agreements with each Direct Clearer that will exchange ICP files with the RG. These bilateral agreements will specify the ICP file exchange times and the End-of-Day (EOD) ICP File Transmission Notice formats. Within these bilateral agreements, the Direct Clearers will be instructed to send the RG bound ICP files to the Contractor and not to the RG.

A.7.5 RG Cheque Image Exchange Process Flow

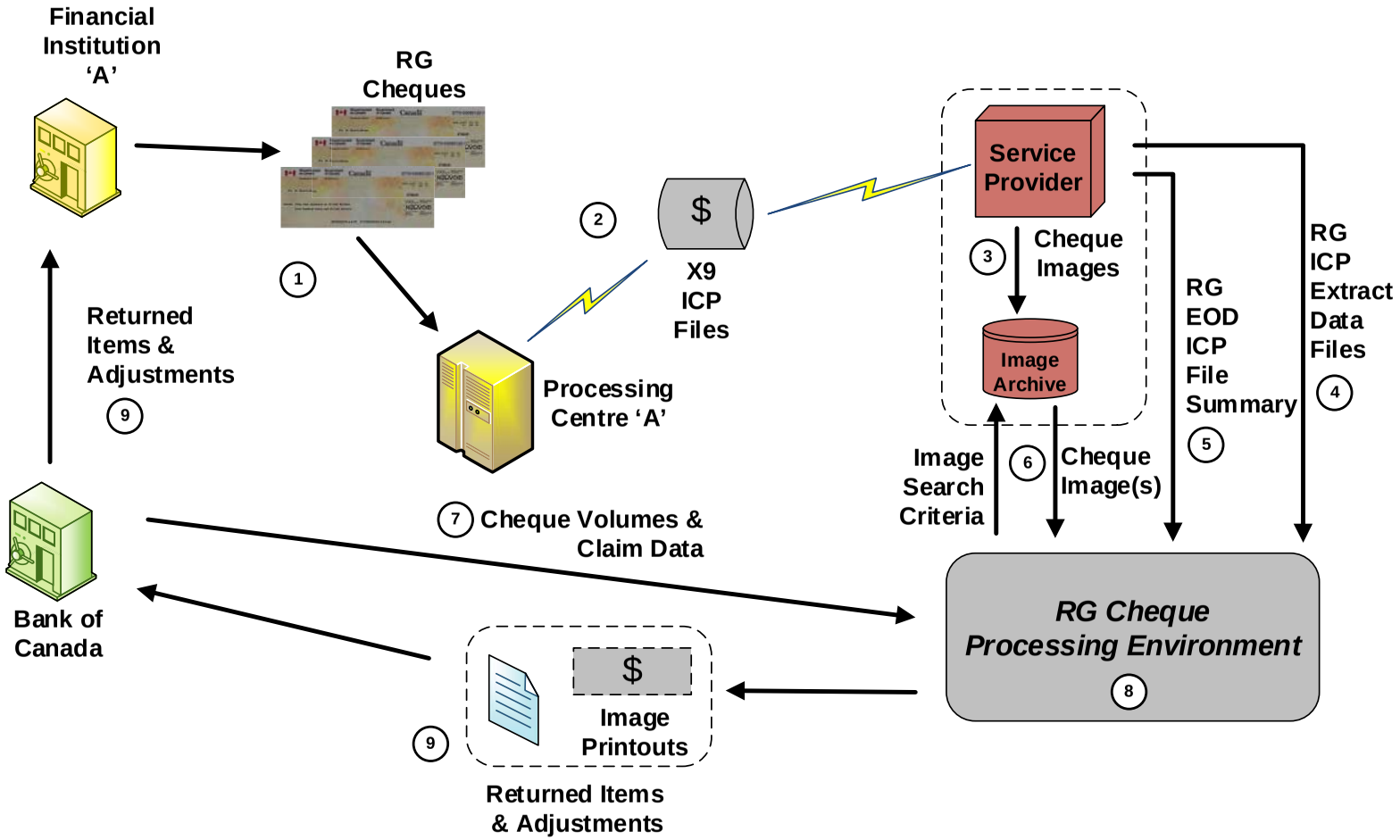
The diagram on the following page illustrates how the cheque images are integrated into the overall process flow for RG cheque redemption and reconciliation. The numbers in the narrative below correspond to the circled numbers on the diagram.

Diagram Key Entities

- Financial Institution ‘A’ – has implemented ICP file functionality
- Processing Centre ‘A’ – item processing facility for Financial Institution ‘A’
- Service Provider – the Contractor that delivers the RG services described in this SOW

1. All the RG cheques cashed at the branches of Financial Institution ‘A’ are transported to their Processing Centre where the items will be imaged. Financial Institution ‘A’ may also transmit cheque images directly to Processing Centre ‘A’.
2. All the images for the RG cheques originating from Financial Institution ‘A’ are formatted into an ICP file which is transmitted to the Service Provider by Processing Centre ‘A’. It may also be possible for Financial Institution ‘A’ to transmit an ICP file directly to the Service Provider.
3. All the images extracted from the ICP files are saved in the Image Archive. The images are indexed to facilitate ease of access by GC personnel.
4. The essential data elements are extract from each ICP file and reformatted into an RG ICP Extract Data File. The RG ICP Extract Data Files are transmitted to PSPC for processing by the RG’s cheque redemption and reconciliation applications.
5. After the last ICP file exchange, the Service Provider will send an RG EOD ICP File Summary listing all the ICP files received, successfully processed and the data sent to the RG for that processing day.
6. GC personnel can query the Image Archive and retrieve, display and/or print an image. GC personnel can also update specific MICR line data fields.
7. The Bank of Canada transmits to the RG, the daily expected volume of RG cheques and the redemption claim amounts submitted by the Direct Clearers against the GC.
8. The RG’s cheque reconciliation application will perform all the item reconciliation edits and verifications.
9. If an exception is encountered during the item reconciliation process, CRCD staff will investigate the situation. If the results of the investigation determine that the item must be returned to the negotiating institution, CRCD staff prepare the necessary paperwork. Any returned cheques, that have been imaged, will be sent as an image printout along with the necessary debit/credit adjustment forms and any related correspondence. The Bank of Canada will redistribute the returned items and adjustments to the appropriate financial institution.

RG Cheque Image Exchange Process Flow



A.7.6 Image Files

1. The Contractor must have the capability of receiving ICP files containing RG items from other Direct Clearers or Clearing Agents.
2. The Contractor must have the capability of providing an acknowledgment of ICP file receipt to the sending Direct Clearer or Clearing Agent (*as per Payments Canada Rule A1 - Section 26*).
3. The Contractor must have the capability of validating the format and completeness of an ICP file at both the file level and the item level.
4. The Contractor must have the automated capability of verifying the image quality and image usability. *(refer to Section A.7.8 – Image Quality and Usability)*
5. The Contactor must have the automated capability of correcting unreadable MICR digits *(refer to Section A.7.9 – MICR Line Corrections)* and detecting incorrectly scanned Cheque Form Numbers *(refer to Section A.7.10 – Incorrectly Scanned Cheque Form Numbers).*
6. The Contractor must have the capability of creating a rejected ICP file notification when either the entire file has format or integrity issues, or the count of items with format or integrity issues exceeds a predetermined threshold. The Contractor must have the capability of sending the rejected ICP file notification to the sending Direct Clearer or Clearing Agent (*as per Standard 015 – Section 7.3)* (*refer to Section A.7.11 – Rejected ICP File Notification).*
7. The Contractor must provide, to the RG, an RG EOD ICP File Summary that lists all ICP files received from the Direct Clearers and Clearing Agents and successfully processed for that day (*refer to Section A.7.12 – RG EOD ICP File Summary).*
8. The Contractor must provide the capability to extract the RG required data elements from the ICP files and populate the '*RG ICP Extract Data File'* (*refer to Section A.7.28 - RG ICP Extract Data File Layout).* The file naming conventions will be negotiated at a later date.
9. The Contractor must provide the capability to store all images received on accepted ICP files in an image archive.
10. For each image set (*front image and back image*) stored in the image archive, the Contractor must generate and assign a unique Item Locator Number (ILN) to the image. The ILN must be provided to the RG on the '*RG ICP Extract Data File'.* The format of the ILN is *YYJJJnnnnnn* where *YYJJJ* is the Julian date format of the current processing cycle date and *nnnnnn* is a sequential number starting at *000001* on each processing day.
11. With each image, at a minimum, the following data elements from the ICP file must also be stored along with the image:
    - Delivering Direct Clearer
    - Processing Cycle Date
    - Item Locator Number (ILN)
    - Cheque Form Number (CFN)
    - Cheque Amount
12. For each ICP file received from a Direct Clearer or Clearing Agent, and successfully processed by the Contractor, the Contactor will format and send one RG ICP Extract Data File.

A.7.7 Image Archive

1. The Contractor must maintain an image archive that will hold all images of RG items for the images received by the Contactor from the other Direct Clearers or Clearing Agents.
2. The Contractor must ensure that the images can be retrieved using various indexes:
    - Primary Index: Item Locator Number (ILN)
    - Secondary Index: Cheque Form Number (CFN)
    - Secondary Index: a combination of Delivering Direct Clearer, Processing Cycle Date Range and/or Cheque Amount

    It should be noted that for other than a search on ILN, multiple images may be retrieved.
3. The Contractor must provide the capability such that the RG can retrieve and display an image from an RG online application within the PSPC technical environment, this would include system documentation in the event the RG wants to integrate direct access to the image archive within the RG's applications.
4. The Contractor must provide training materials, in both official languages, on how to use the Contractor's image archive service.
5. The Contractor must ensure that the image archive has redundant copies of all images in order to prevent image loss in the event there is hardware and/or electronic storage device failures.
6. The Contractor must ensure that the image archive has the required security and data segregation mechanisms in place to prevent unauthorized or accidental access to images of RG items.
7. The Contractor must ensure that the image archive is a key component within the business continuity and disaster recovery plan.
8. The Contactor must provide the capability for authorized Government of Canada personnel to have online access to the image archive to view RG imaged items.
9. The Contactor must provide the capability for authorized Government of Canada personnel to create an image printout of an RG imaged item. On each image printout, the printout must also include the Item Locator Number (ILN).
10. The Contactor must provide the capability for authorized Government of Canada personnel to have online access to update the Cheque Form Number and Cheque Amount data elements associated with an image.
11. The Contractor must ensure that the image archive is available to authorized Government of Canada personnel during the processing hours of the Cheque Redemption Control Directorate (CRCD) staff in Matane, Quebec (*refer to Section A.7.22 – CRCD Hours of Operation).*
12. The current image archive maintained at the CRCD cheque facility is not included in the proposed solution being requested (i.e. the CRCD images will not be migrated to the new image archive).

A.7.8 Image Quality and Usability

As per the Payments Canada Image Rules, all images must be usable. A usable image is a digital representation of the front and back of a payment item where any field or portion that would be required to be present and legible (read or deciphered by a human) on the original payment item (e.g. MICR line) is present and legible on the image, and any field or portion that would be required to be present and viewable (seen without obstruction) on the original payment item (e.g. signature) is present and viewable on the image.

The Contractor must apply an automated process to ensure that all images of RG items are usable. Any image that is either missing or deemed not usable must be flagged on the cheque details record sent to the RG.

A.7.9 MICR Line Corrections

On occasion a MICR line digit will not be readable. When this occurs, the cheque data record received on the ICP file will have the unreadable characters replaced by asterisks ('*'). As previously noted, within the MICR line on RG warrants, the Transit Number is always '*00000'* and the Financial Institution is always '*117'*. The MICR line on RG warrants does not use a Serial Number nor a Transaction Code.

To ensure that the highest quality data is forwarded to the RG, the Contractor must correct any unreadable characters found in the RG Cheque Form Number (On-Us field) and the Cheque Amount.

The Contractor must implement processes that:

- detect the presence of unreadable characters within a cheque detail data record
- visually present the item to a trained operator
- correct the unreadable characters (*On-Us and Cheque Amount fields only*)
- continue with all subsequent processes involving the data and image with the corrected data
- flag the cheque detail records where the MICR line was corrected

This process cannot impact the service timelines for delivery of the RG ICP Extract Data File to the RG.

A.7.10 Incorrectly Scanned Cheque Form Numbers

On occasion, the Cheque Form Number (CFN) within the MICR line has no digits considered unreadable but nevertheless is incorrectly scanned. The incorrect CFN number is then passed with the image and cheque details. In order to reduce the number of these errors sent onto the RG's cheque reconciliation application, the Contractor must make best efforts to detect and correct these situations.

As noted in *Section A.2 RG Cheques*, the RG's CFN is printed in the upper right corner of the cheque face and within the MICR line also on the cheque face. The Contractor must implement a process that ensures that the CFN within the extracted MICR line data matches the CFN in the upper right corner. This CFN is considered the correct number as the MICR line CFN may have been the cause of the incorrect scanned number.

The Contractor must ensure that their CFN matching algorithm achieves a high level of confidence before altering the CFN within the MICR line data. For any item where an incorrectly scanned CFN was corrected must be flagged on the cheque details record sent to the RG.

A.7.11 Rejected ICP File Notification

As per Payments Canada Rule A10 Section 29, in the event that the receiving Direct Clearer rejects an ICP file, a notice of file rejection must be sent to the delivering Direct Clearer. The format, media, and method of communication will be specified within the bilateral agreements between the RG and each Direct Clearer. The RG will endeavor to standardize the method of file rejection notices across all bilateral agreements. In addition to sending the file reject notice to the delivering Direct Clearer, the Contactor must send a copy of the notice to CRCD and to the RG systems management group located in Gatineau, Quebec.

The file reject notice must include the following information:

- Processing Cycle Date
- File Rejection Date
- File Rejection Time
- Delivering Direct Clearer
- ICP File Name
- Reason For Rejection

Any headings and literals within the file reject notification must be presented in both official languages. The transmission method and destination of the Rejected ICP File Notification will be confirmed if and when a contract is awarded.

A.7.12 RG EOD ICP File Summary

Following the transmission of the last RG ICP Extract File to the RG for that processing day, the Contractor must send an RG EOD ICP File Summary to the RG (*refer to Section A.7.29 - RG EOD ICP File Summary).* The summary data must be provided in electronic format and include, at a minimum, the following data elements:

- Processing Cycle Date
- For each Direct Clearer:
  For each ICP File received from that Direct Clearer:
  - ICP File Name
  - Number of Items on the ICP File
  - Total Value of the ICP File

  Total Number of Items from all ICP Files from that Direct Clearer
  Total Value of all ICP Files from that Direct Clearer

Any headings and literals within the file summary must be presented in both official languages. The transmission method and destination of the RG EOD ICP File Summary will be confirmed if and when a contract is awarded.

A.7.13 Return Replacement Documents (RRD)

The RG is planning to use image printouts when payment is refused and is returned to the negotiating financial institution (*refer to Step 9 in Section A.7.5 RG Cheque Image Exchange Process Flow*). However, it is expected that the use of RRDs would be a more efficient method of returning items (*refer to Payments Canada Standard 013*). In order to create an RRD, additional data from the ICP file will be required to be stored with the image (e.g. Return Location Routing Number).

The RG would be interested in a process that would:

- allow an authorized CRCD staff member to retrieve an image from the archive
- provide a return reason code
- request an RRD print
- the Contactor would provide the functionality to format the RRD as per Standard 013
- the CRCD staff member would print the RRD on a MICR printer located in the CRCD facility

A.7.14 Item Threshold Alert

The daily labour workforce required in CRCD depends on the volume of reconciliation exceptions and investigations that need to be processed. In order to ensure that adequate staff are available to handle the expected workload, CRCD requires advance notice of the incoming volume of items.

Once the Contractor has received 100,000 items, within a processing day, that are to be delivered to the RG, the Contractor must notify CRCD that this threshold has been reached. The method of communication (e.g. telephone or e-mail) for this notification will be negotiated at a later date.

A.7.15 Fraud Detection and Prevention

The RG has great interest in reducing the taxpayer burden which is a result of altered and counterfeit Government cheques. At this time there are no specific requirements that the Contractor must meet. However, following contract award, it is expected that Contractor propose and explore possible solutions with the RG that will help detect and prevent cheque fraud.

A.7.16 Business Continuity and Disaster Recovery Site

1. The Contractor must ensure that business continuity plans and procedures are in place in the event that a situation interrupts the course of normal business. The business continuity plans must ensure that any interruption in service does not last longer than 4 hours.
2. The Contractor must follow any contingency procedures that have already been establish by Payments Canada (*as per Rule A10 – Part V).*
3. The Contractor must ensure that a disaster recovery site is established and functional (*as per Rule A10 – Sections 20 & 21*).
4. On an annual basis the Contractor must test their disaster recovery plan, the Contractor must agree to include the transmission of files to the RG's production environment during the Contactor's disaster recovery testing to ensure connectivity between the Contractor's disaster recovery site and the RG's production environment.
5. The Contactor must agree to participate in the RG's disaster recovery plans by transmitting files, when requested, to the RG's disaster recovery site from the Contactor's production environment to ensure connectivity between the Contractor's production environment and the RG's disaster recovery site. The RG's disaster recovery testing not to be conducted more than once a year.

A.7.17 Data Sovereignty

1. The Contractor must agree and acknowledge that the Contractor is a custodian of the RG's cheque image data, however the Government of Canada remains the legal owner of the cheque data and images.

2. The Contractor must agree and acknowledge that it is a mandatory condition that all of the RG's cheque image data must remain within Canada when the data is in transit and when the data is at rest.

A.7.18 Data Network

1. The Contractor must ensure that all RG cheque data and images are transmitted within a secure environment.
2. The Contractor must ensure that the transmission of all data is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or unauthorized replay.
3. The Contractor must ensure that all data sent to the RG is transmitted using the Payments Canada's CPA Services Network (CSN).
4. The Contractor must ensure that the Contractor has their own CSN Node or the authorized use of a CSN Node.

A.7.19 Data Retention

1. The Receiver General will have the right to specify the minimum and maximum data retention periods. When the required data retention period has passed, the data must be destroyed or erased. The Contractor must develop guidelines and implement procedures to govern the destruction of the data which are to be approved by the RG. These guidelines and procedures must prevent unauthorized access during the destruction of the data.
2. The Contractor must retain all ICP files received from the Direct Clearers for a period of 120 calendar days.
3. The Contactor must provide the capability to retain RG cheque images for a minimum period of 7 years.
4. Due to the need to investigate items, the 7 year period will re-commence from the date when the image was last accessed.
5. All RG owned data that is held by the Contractor must be deleted according to a regular schedule that follows the stated retention periods.
6. If the Contractor must remove storage media from the Contractor's secure environment that may have been used to store RG data, if the storage media can be overwritten it must be sanitized through a secure software overwrite, or if the storage media cannot be overwritten it must be physically destroyed.
7. Following the purging of ICP files, cheque images, and any other RG data held by the Contractor, the Contactor must provide notification to the RG to confirm that the data has been deleted and list the date range(s) for which the information is no longer available.

A.7.20 Points of Contact

1. The Contractor must identify personnel to fill two key roles that will be used as points of contact with the RG. These roles include:

    - Executive Sponsor: The Contractor must provide an Executive Sponsor for the Contract. The Executive Sponsor will have overall responsibility, on behalf of the Contractor, for all obligations under the Contract. The Executive Sponsor must be at a senior management level within the

Contractor's organization. The Executive Sponsor will be an escalation point for issues that cannot be resolved by the Contract Manager.

- Contract Manager: The Contractor must provide a Contract Manager as its representative responsible, at an operational level, for successfully delivering the solution under the contract as well as the business relationships between the RG and the Contractor.

2. The RG will assign a Project Manager to act as its point of contact for all matters concerning the initial implementation of the cheque image exchange solution and to handle on-going operations and problem escalation & resolution.

A.7.21 Implementation

1. The Contractor must provide a detailed implementation plan listing all activities, durations and dependencies required to implement the RG's cheque image exchange solution.
2. The Contractor must include testing activities involving the RG's participation, the RG must agree with the timing and duration of these testing activities.
3. The RG reserves the right to request amendments to the implementation plan.
4. The Contractor must complete all activities within the timeframes stipulated in the final approved implementation plan unless agreement is obtained from the RG to alter the plan.
5. The Contractor must obtain final approval from the Receiver General prior to live implementation of the cheque image exchange solution.
6. Specific implementation activities must begin after the date of contract award, these activities must include:

    - within 5 business days of contract award (unless otherwise mutually agreed), provide a list of contact names and contact information for the Contactor's representatives who will handle the implementation and set-up activities
    - within 10 business days of contract award (unless otherwise mutually agreed), participate in operational and technical team meetings and/or teleconferences
    - within 15 business days of contract award (unless otherwise mutually agreed), present an implementation plan that details all testing, configuration, training and deployment activities

A.7.22 CRCD Hours of Operation

The processing hours of the Cheque Redemption Control Directorate (CRCD) staff in Matane, Quebec are as follows (excluding GC statutory holidays):

- Monday, Tuesday, Wednesday and Saturday: 07:00am to 19:00pm EST
- Thursday and Friday: 07:00am to 22:00pm EST

A.7.23 Ongoing Operations

1. The Contractor must be responsible for the day-to-day operational activities required to support effective management of the cheque image exchange service and the production environment in which it operates. These activities include, but are not limited to, system availability and performance,

problem management, incident management, change management, communication and escalation procedures, and regular management reporting.

2. The Contractor must also interface with the direct clearers and their processing agents with respect to cheque image exchange activities, issues and enquiries.

3. The Contactor must provide a process to record and track reported problems and incidents. The Contractor must provide the contact names and contact information for the Contactor's representatives who will handle any issues with the cheque imaging service, as well as the second and third level escalation contacts. The Contractor must provide the expected and maximum turnaround times for responding to, and resolution of, reported problems and incidents.

4. The Contractor must provide the contact names and contact information for the authorized personnel responsible for daily operations, security issues and technical support.

5. The Contractor must ensure that qualified, technical support personnel are available during the processing hours of the Cheque Redemption Control Directorate (CRCD) staff in Matane, Quebec (*refer to Section A.7.22 – CRCD Hours of Operation).* The support personnel provided by the Contractor must be bilingual.

A.7.24 Service Standards

1. The service standards and the respective performance levels will specify the Contractor's minimum performance to meet the RG's business requirements. Accordingly, the service standards:
   - must be regularly reviewed by the Contractor and the RG;
   - must be subject to various corrective measures and continuous improvement objectives;
   - may include additions, amendments, and deletions during the term of the contract, within the scope of the contract.
2. The Contractor must, unless otherwise agreed with the RG, commence measuring its service levels from the date the cheque image exchange solution goes live in the production environment.
3. The Contractor must at its own cost, take appropriate corrective measures when service standards are not met.
4. The RG must receive the corresponding RG ICP Extract Data File within two (2) hours after the Contactor has received an accepted ICP file from the delivering Direct Clearer.
5. The Contractor must ensure that all images from the successfully processed ICP files for a given processing day, are stored in the Image Archive by 6:00am EST the following business day.
6. The Contactor must ensure that an image is available from the Image Archive to be viewed and/or printed, on average, within five (5) seconds after requesting the image.
7. The Contractor must ensure that the expected turnaround times for the responding to, and resolution of, reported problems and incidents are met 80% of the time.

A.7.25 Change Management

The Contractor must follow a formal and proven change management process that is designed to evaluate and minimize risks when implementing system changes and/or upgrades. The Contactor must agree that

their change management process is based on a framework that includes, at a minimum, the following processes and procedures:

- clearly defined business and technical objectives, requirements and benefits
- an articulated options analysis and any associated risks
- establish and monitor a detailed work plan
- regularly scheduled status meetings with all stakeholders
- identify and provide any needed training and updated documentation
- ensure that thorough testing is conducted in a dedicated testing environment, all defects are corrected and re-tested
- ensure that each deployment includes a back-out plan
- the appropriate signoffs before deploying into the production environment

A.7.26 Contract Transition Period

When this contract is resolicited, and should there be a new contractor, the current contractor, must facilitate the transition to the new contractor. This includes, but is not limited to, the migration of all cheque image data to the RG's new contractor. The Contractor must also provide the RG and the new contractor with the information necessary to map the existing cheque image exchange service to any new solution.

A.7.27 Languages of Operation

The Contractor must ensure that all online interfaces and any related documentation that will be used by GC personnel are bilingual and are available in both official languages of Canada (English and French).

A.7.28 RG ICP Extract Data File Layout

1. The file layout described in this section is required in this format to ensure that minimal modifications are necessary to the current suite of RG cheque reconciliation and redemption applications.
2. The file and record layout shown below describes the data and format that the Contractor must transmit to the RG for all ICP items processed by the Contractor.
3. There should be one (1) RG ICP Extract Data File for each ICP file successfully processed by the Contractor.
4. The RG ICP Extract Data File contains the RG required data extracted from the original ICP file.

File Header			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '01'	Record 01 Field 01
Destination Routing Number	Char(09)	format 'CP00RSNNN'	Record 01 Field 04
Origin Routing Number	Char(09)	format 'CP00RSNNN'	Record 01 Field 05
X9 File Creation Date	Char(08)	format 'YYYYMMDD'	Record 01 Field 06
X9 File Creation Time	Char(14)	format ''YYYYMMDDHHMNSS'	Record 01 Field 07
File Creation Time	Char(14)	format ''YYYYMMDDHHMNSS'	Derived – Note 1

Note 1: File Creation Time - The timestamp when the RG ICP Extract Data File was created from the original X9 ICP file sent by the delivering direct clearer

Cash Letter Header			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '10'	Record 10 Field 01
Destination Routing Number	Char(09)	format 'CP00RSNNN'	Record 10 Field 03
Cash Letter Business Date	Char(08)	format 'YYYYMMDD'	Record 10 Field 05
Cash Letter Id	Char(08)		Record 10 Field 10

Bundle Header			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '20'	Record 20 Field 01
Bundle Id	Char(10)		Record 20 Field 07
Bundle Sequence Number	Char(04)		Record 20 Field 08

Cheque Detail			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '25'	Record 25 Field 01
On-Us	Char(20)		Record 25 Field 06
Cheque Amount	Numeric(10)	format '$$$$$$$$.99'	Record 25 Field 07
Item Sequence Number	Char(15)		Record 25 Field 08
Item Locator Number	Numeric(11)	YYJJJnnnnnn	Derived – Note 2
Image Validation Indicator	Char(01)	Value '0' (valid) '1' (MICR line correction) '2' (incorrectly scanned MICR CFN corrected) '3' (image is missing) '4' (image is unusable)	Derived – Note 3

Note 2: Item Locator Number – The unique item number assigned by the Contactor for each image set (*front image and back image*) stored in the image archive.

Note 3: Image Validation Indicator – An indicator used to denote that there were problems detected with the image(s) delivered on the ICP file.

'0' – no problems encountered with the front or back images
'1' – the MICR line data was received from the Direct Clearer with unreadable digits and was corrected
'2' – the MICR data CFN was found to be incorrectly scanned and was corrected
'3' – no front or back image was included on the ICP file for an item
'4' – either the front and/or back image of an item is not usable

Bundle Trailer			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '70'	Record 70 Field 01
Bundle Item Count	Numeric(04)	format '9999'	Record 70 Field 02
Bundle Total Amount	Numeric(12)	format '$$$$$$$$$$.99'	Record 70 Field 03

Cash Letter Trailer			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '90'	Record 90 Field 01
Cash Letter Item Count	Numeric(08)	format '99999999'	Record 90 Field 03
Cash Letter Item Value	Numeric(14)	format '$$$$$$$$$$$$.99'	Record 90 Field 04

File Trailer			
Data Element	**Data Type**	**Format**	**X9 File Source**
Record Type	Char(02)	value '99'	Record 99 Field 01
Total Record Count	Numeric(08)	format '99999999'	Record 99 Field 03
Total Item Count	Numeric(08)	format '99999999'	Record 99 Field 04
Total File Value	Numeric(16)	format '$$$$$$$$$$$$$$.99'	Record 99 Field 05

5. The RG ICP Extract Data File has the following structure:

File Header (Record Type '01')
Cash Letter Header (Record Type '10') *(first Cash Letter record)*
Bundle Header (Record Type '20') *(first Bundle record within the Cash Letter)*
Cheque Detail (Record Type '25') *(first Cheque Detail record with the Bundle)*
……
Cheque Detail (Record Type '25') *(last Cheque Detail record with the Bundle)*
Bundle Trailer (Record Type '70') *(first Bundle Trailer record within the Cash Letter)*
……
Bundle Header (Record Type '20') *(last Bundle record within the Cash Letter)*
Cheque Detail (Record Type '25') *(first Cheque Detail record with the Bundle)*
……
Cheque Detail (Record Type '25') *(last Cheque Detail record with the Bundle)*
Bundle Trailer (Record Type '70') *(last Bundle Trailer record within the Cash Letter)*
Cash Letter Trailer (Record Type '90') *(first Cash Letter Trailer record)*
……
Cash Letter Header (Record Type '10') *(last Cash Letter record)*
Bundle Header (Record Type '20') *(first Bundle record within the Cash Letter)*
Cheque Detail (Record Type '25') *(first Cheque Detail record with the Bundle)*
……
Cheque Detail (Record Type '25') *(last Cheque Detail record with the Bundle)*
Bundle Trailer (Record Type '70') *(first Bundle Trailer record within the Cash Letter)*
……
Bundle Header (Record Type '20') *(last Bundle record within the Cash Letter)*

Cheque Detail (Record Type '25') *(first Cheque Detail record with the Bundle)*
……
Cheque Detail (Record Type '25') *(last Cheque Detail record with the Bundle)*
Bundle Trailer (Record Type '70') *(last Bundle Trailer record within the Cash Letter)*
Cash Letter Trailer (Record Type '90') *(last Cash Letter Trailer record)*
File Trailer (Record Type '99)

The RG may request amendments or revisions to the file layout during the contract period, the implementation timing of any such modifications will be negotiated with the Contractor.

A.7.29 RG EOD ICP File Summary

1. The RG EOD ICP File Summary lists all ICP files received from the Direct Clearers and Clearing Agents that were successfully processed for a given processing day.

File Header		
Data Element	**Data Type**	**Format**
Record Type	Char(02)	value '01'
Processing Cycle Date	Char(08)	format 'YYYYMMDD'
File Creation Time	Char(14)	format ''YYYYMMDDHHMNSS'

ICP File		
Data Element	**Data Type**	**Format**
Record Type	Char(02)	value '02'
Delivering Direct Clearer	Numeric(03)	format '999'
ICP File Name	Char(44)	
ICP File Item Count	Numeric(08)	format '99999999'
ICP File Item Value	Numeric(16)	format '$$$$$$$$$$$$$.99'

Direct Clearer Totals		
Data Element	**Data Type**	**Format**
Record Type	Char(02)	value '03'
Delivering Direct Clearer	Numeric(03)	format '999'
Total File Count	Numeric(03)	Format '999'
Total Item Count	Numeric(08)	format '99999999'
Total Item Value	Numeric(16)	format '$$$$$$$$$$$$$.99'

2. The RG EOD ICP File Summary has the following structure:

File Header (Record Type '01')
ICP File (Record Type '02') *(first ICP file record for the first direct clearer)*

……
ICP File (Record Type ’02’) *(last ICP file record for the first direct clearer)*
Direct Clearer Totals (Record Type ‘03’) *(totals record for the first direct clearer)*
……
ICP File (Record Type ’02’) *(first ICP file record for the last direct clearer)*
……
ICP File (Record Type ’02’) *(last ICP file record for the last direct clearer)*
Direct Clearer Totals (Record Type ‘03’) *(totals record for the last direct clearer)*

The RG may request amendments or revisions to the file layout during the contract period, the implementation timing of any such modifications will be negotiated with the Contractor.

A.8 RG Cheque Volumes

The following table provides the actual and forecasted volumes of RG issued cheques. It is anticipated that the volume of cheques will decline over the years as the GC continues to promote direct deposit as the preferred method of payment.

These estimates have been provided to illustrate expected future volumes, there is no guarantee that these predictions will materialize.

Actual	Fiscal Year	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Annual	Decrease
	2014-2015	8,017,301	6,950,628	4,145,066	6,934,490	3,701,478	3,178,218	5,789,820	2,832,493	3,464,238	4,661,939	2,569,686	3,541,232	55,786,589	
	2015-2016	6,213,522	4,978,604	3,199,639	5,924,346	3,182,090	3,106,775	4,773,348	2,656,503	2,905,995	3,948,256	2,443,944	3,344,931	46,677,953	16.33%
	2016-2017	5,418,877	4,451,286	3,531,964	4,453,715	2,234,159	1,739,340	3,168,382	1,902,414	1,544,266	3,548,664	1,781,496	2,481,602	36,256,165	22.33%
	2017-2018	4,264,244	4,260,392	2,336,753	3,863,277	2,300,669	1,570,904	3,367,259	1,940,776	1,509,511	3,433,312	1,681,764	1,918,227	32,447,088	10.51%
	2018-2019	4,442,047	4,051,952	2,109,810	3,763,773	2,210,071	1,974,564	3,118,939	1,437,295	1,480,273	3,082,567	1,420,697	1,986,893	31,078,881	4.22%
	Average	5,671,198	4,938,572	3,064,646	4,987,920	2,725,693	2,313,960	4,043,550	2,153,896	2,180,857	3,734,948	1,979,517	2,654,577	40,449,335	

Forecast	Fiscal Year	Annual	Decrease
	2019-2020	30,000,000	3.47%
	2020-2021	29,000,000	3.33%
	2021-2022	28,000,000	3.45%
	2022-2023	27,000,000	3.57%
	2023-2024	26,000,000	3.70%

A.9 RG Cheque Image Volumes

To ensure that all processes in the cheque image exchange service are functioning properly, the RG will implement using a phased approach. The RG will onboard the Direct Clearers as the bilateral agreements are made with those Direct Clearers who have implemented ICP file functionality.

The following table provides the estimated volume of images that will be delivered to the Contractor on behalf of the RG.

These estimates have been provided to illustrate expected future volumes, there is no guarantee that these predictions will materialize.

Fiscal Year	Estimated Number of Cheques	Estimated Number of Images	
		Between	And
2019-2020	30,000,000		
2020-2021	29,000,000	0	5,800,000
2021-2022	28,000,000	5,600,000	12,320,000
2022-2023	27,000,000	11,888,000	17,280,000
2023-2024	26,000,000	16,640,000	26,000,000

A.10 RG Cheque Return Volumes

The following table provides the estimated volume of cheques that will be returned by the RG to the negotiating financial institutions.

It should be noted that the estimates of return volumes currently include items that are returned due to CRD quality, encoding errors and printed duplicates. It is expected that implementing an image exchange solution will result in a decrease in the volumes related to those types of issues.

These estimates have been provided to illustrate expected future volumes, there is no guarantee that these predictions will materialize.

Fiscal Year	Estimated Number of Cheques	Estimated Number of Returns
2019-2020	30,000,000	75,282
2020-2021	29,000,000	72,772
2021-2022	28,000,000	70,263
2022-2023	27,000,000	67,754
2023-2024	26,000,000	65,244

A.11 User Access – Image Archive

The following table provides the number of RG staff that will require access to the Contractor's image archive.

	User Count
Total number of users requiring image archive access	**70**
Average number of users working during a shift	**40**

It should be noted that all users working within the same shift will not be simultaneously accessing the image archive. Typically the image archive will only be accessed if an item is flagged as an exception and investigation activities are required.

ANNEX B

QUESTIONS AND INFORMATION REQUESTS

B.1 Questions

The respondents are requested to review the SOW and provide detailed answers to the following questions:

1. Are there any requirements for the RG's cheque image exchange solution as stated within the SOW that are not clear or that your organization would be unable to provide?

2. Is there any additional information needed in order for your organization to be able to prepare a response to a future RFP for this service?

3. Are there any IT security requirements that are not clear or that your organization would be unable to demonstrate compliance?

B.2 Pricing

The RG is seeking feedback from industry regarding price estimates. Any feedback provided will not be disclosed to any other parties, nor will it be used to evaluate bidders under any subsequent solicitation process.

If an RFP is published in the future, the RG will be expecting a firm all-inclusive cheque image unit price for the services described in the SOW. Estimated volume forecasts are provided in the SOW (Sections A.8 through A.11).

1. Would your organization be able to provide an estimated all-inclusive cheque image unit price at this time?

2. In Section A.7.13 of the SOW, the use of Return Replacement Documents (RRD) is mentioned as a possible process improvement instead of the use of Image Printouts. Would the implementation of the RRD process described in this section significantly impact the unit price? (please respond even if a unit price is not provided at this time)

3. Would any of the processes as described in the SOW have a significant impact on your organization's proposed unit price? (please respond even if a unit price is not provided at this time)

ANNEX C

IT SECURITY CONTROLS PROFILE

Summary

The table below provides all of the security control families that are suitable for GC departments engaged in business activities of very low to very high sensitivity and criticality in unclassified, protected, and classified domains.

This list has been created as a tool to assist security practitioners, business owners, and project teams in their efforts to protect information systems in compliance with applicable GC legislation and TBS policies, directives, and standards.

Purpose

This list will be used during the RFI (Request for Information) stage to convey enough information to the bidders in relation to the security controls requirements that will be expected to be satisfied after contract has been awarded. Additional control enhancements (an example is provided following the table) may be added during RFP (Request for Proposal) for protecting information technology systems and managing IT security risks.

FAMILY	CHILD
ACCESS CONTROL (AC)	AC-1 Access control policy and procedures AC-2 Account management AC-3 Access enforcement AC-4 Information flow enforcement AC-5 Separation of duties AC-6 Least privilege AC-7 Unsuccessful login attempts AC-8 System use notification AC-9 Previous logon (access) notification AC-10 Concurrent session control AC-11 Session lock AC-12 Session termination AC-13 Supervision and review — access control AC-14 Permitted actions without identification or authentication AC-15 Automated marking AC-16 Security attributes AC-17 Remote access AC-18 Wireless access AC-19 Access control for mobile devices AC-20 Use of external information systems AC-21 User-based collaboration and information sharing AC-22 Publicly accessible content AC-23 Data mining protection AC-24 Access control decisions AC-25 Reference monitor

AWARENESS AND TRAINING (AT)	AT-1 Security awareness and training policy and procedures AT-2 Security awareness AT-3 Role based security training AT-4 Security training records AT-5 Contacts with security groups and associations
AUDIT AND ACCOUNTABILITY (AU)	AU-1 Audit and accountability policy and procedures AU-2 Auditable events AU-3 Content of audit records AU-4 Audit storage capacity AU-5 Response to audit processing failures AU-6 Audit review, analysis, and reporting AU-7 Audit reduction and report generation AU-8 Time stamps AU-9 Protection of audit information AU-10 Non-repudiation AU-11 Audit record retention AU-12 Audit generation AU-13 Monitoring for information disclosure AU-14 Session audit AU-15 Alternate audit capability AU-16 Cross-organizational auditing
SECURITY ASSESSEMENT AND AUTHORIZATION (CA)	CA-1 Security assessment and authorization policies and procedures CA-2 Security assessments CA-3 Information system connections CA-4 Security certification CA-5 Plan of action and milestones CA-6 Security authorization CA-7 Continuous monitoring CA-8 Penetration testing CA-9 Internal system connections
CONFIGURATION MANAGEMENT (CM)	CM-1 Configuration management policy and procedures CM-2 Baseline configuration CM-3 Configuration change control CM-4 Security impact analysis CM-5 Access restrictions for change CM-6 Configuration settings CM-7 Least functionality CM-8 Information system component inventory CM-9 Configuration management plan CM-10 Software usage restrictions CM-11 User installed software
CONTINGENCY PLANNING (CONTINUITY PLANNING) (CP)	CP-1 Contingency planning policy and procedures CP-2 Contingency plan CP-3 Contingency training CP-4 Contingency plan testing and exercises CP-5 Contingency plan update CP-6 Alternate storage site CP-7 Alternate processing site CP-8 Telecommunications services CP-9 Information system backup CP-10 Information system recovery and reconstitution CP-11 Alternate communications protocols CP-12 Safe mode

	CP-13 Alternative security mechanisms
IDENTIFICATION AND AUTHENTICATION (IA)	IA-1 Identification and authentication policy and procedures IA-2 Identification and authentication (organizational users) IA-3 Device identification and authentication IA-4 Identifier management IA-5 Authenticator management IA-6 Authenticator feedback IA-7 Cryptographic module authentication IA-8 Identification and authentication (non-organizational users) IA-9 Service identification and authentication IA-10 Adaptive identification and authentication IA-11 Re-authentication
INCIDENT RESPONSE (IR)	IR-1 Incident response policy and procedures IR-2 Incident response training IR-3 Incident response testing and exercises IR-4 Incident handling IR-5 Incident monitoring IR-6 Incident reporting IR-7 Incident response assistance IR-8 Incident response plan IR-9 Information spillage response IR-10 Integrated information security analysis team
MAINTENANCE (MA)	MA-1 System maintenance policy and procedures MA-2 Controlled maintenance MA-3 Maintenance tools MA-4 Non-local maintenance MA-5 Maintenance personnel MA-6 Timely maintenance
MEDIA PROTECTION (MP)	MP-1 Media protection policy and procedures MP-2 Media access MP-3 Media marking MP-4 Media storage MP-5 Media transport MP-6 Media sanitization MP-7 Media use MP-8 Media downgrading
PLANNING (PL)	PL-1 Security planning policy and procedures PL-2 System security plan PL-3 System security plan update PL-4 Rules of behaviour PL-5 Privacy impact assessment PL-6 Security-related activity planning PL-7 Security concepts of operation PL-8 Information security architecture PL-9 Central management
RISK ASSESSMENT (RA)	RA-1 Risk assessment policy and procedures RA-2 Security categorization RA-3 Risk assessment RA-4 Risk assessment update RA-5 Vulnerability scanning RA-6 Technical surveillance countermeasures survey
	SA-1 System and services acquisition policy and procedures SA-2 Allocation of resources

SYSTEM AND SERVICES ACQUISITION (SA)	SA-3 System development lifecycle SA-4 Acquisition process SA-5 Information system documentation SA-6 Software usage restrictions SA-7 User-installed software SA-8 Security engineering principles SA-9 External information system services SA-10 Developer configuration management SA-11 Developer security testing SA-12 Supply chain protection SA-13 Trustworthiness SA-14 Criticality analysis SA-15 Development process, standards, and tools SA-16 Developer provided training SA-17 Developer security architecture and design SA-18 Tamper resistance and detection SA-19 Component authenticity SA-20 Customized development of critical components SA-21 Developer screening SA-22 Unsupported system components
SYSTEM AND COMMUNICATIONS PROTECTION (SC)	SC-1 System and communications protection policy and procedures SC-2 Application partitioning SC-3 Security function isolation SC-4 Information in shared resources SC-5 Denial of service protection SC-6 Resource availability SC-7 Boundary protection SC-8 Transmission confidentiality and integrity SC-9 Transmission confidentiality SC-10 Network disconnect SC-11 Trusted path SC-12 Cryptographic key establishment and management SC-13 Cryptographic protection SC-14 Public access protections SC-15 Collaborative computing devices SC-16 Transmission of security attributes SC-17 Public key infrastructure certificates SC-18 Mobile code SC-19 Voice over internet protocol SC-20 Secure name/address resolution service (authoritative source) SC-21 Secure name/address resolution service (recursive or caching resolver) SC-22 Architecture and provisioning for name/address resolution service SC-23 Session authenticity SC-24 Fail in known state SC-25 Thin nodes SC-26 Honeypots SC-27 Platform-independent applications SC-28 Protection of information at rest SC-29 Heterogeneity SC-30 Concealment and misdirection SC-31 Covert channel analysis SC-32 Information system partitioning SC-33 Transmission preparation integrity

	SC-34 Non-modifiable executable programs SC-35 Honeyclients SC-36 Distributed processing and storage SC-37 Out-of-band channels SC-38 Operations security SC-39 Process isolation SC-40 Wireless link protection SC-41 Port and I/O device access SC-42 Sensor capability and data SC-43 Usage restrictions SC-44 Detonation chambers SC-100 Source authentication SC-101 Unclassified telecommunications systems in secure facilities
SYSTEM AND INFORMATION INTEGRITY (SI)	SI-1 System and information integrity policy and procedures SI-2 Flaw remediation SI-3 Malicious code protection SI-4 Information system monitoring SI-5 Security alerts, advisories, and directives SI-6 Security functional verification SI-7 Software, firmware, and information integrity SI-8 Spam protection SI-9 Information input restrictions SI-10 Information input validation SI-11 Error handling SI-12 Information output handling and retention SI-13 Predictable failure prevention SI-14 Non-persistence SI-15 Information output filtering SI-16 Memory protection SI-17 Fail-safe procedures

An example of an additional Control Enhancement that may be added as required:

FAMILY	CHILD	CONTROL	CONTROL ENHANCEMENT
ACCESS CONTROL (AC)	AC-3 ACCESS ENFORCEMENT	(A) The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	(1) ACCESS ENFORCEMENT MANDATORY ACCESS CONTROL The information system enforces mandatory access control policies over all subjects and objects where the policy specifies that: (a) The policy is uniformly enforced across all subjects and objects within the boundary of the information system; (b) A subject that has been granted access to information is constrained from doing any of the following; - Passing the information to unauthorized subjects or objects; - Granting its privileges to other subjects; - Changing one or more security attributes on subjects, objects, the information system, or information system components; - Choosing the security attributes and attribute values to be associated with newly created or modified objects; or - Changing the rules governing access control; and - May explicitly be granted defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.