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 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet ePPT Next Generation	
Solicitation No. - N° de l'invitation B7021-170031/B	**Date** 2017-06-13
Client Reference No. - N° de référence du client B7021-170031	**GETS Ref. No. - N° de réf. de SEAG** PW-$$XS-002-31598
File No. - N° de dossier 002xs.B7021-170031	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-09-11**	**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: Hradecky, Michael	**Buyer Id - Id de l'acheteur** 002xs
Telephone No. - N° de téléphone (819) 420-2212 ( )	**FAX No. - N° de FAX** (819) 997-8303
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** DEPARTMENT OF CITIZENSHIP AND IMMIGRATION 70 CREMAZIE STREET GATINEAU Quebec K1A1L1 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 Operations Support Systems Division/Systèmes de soutien des activités opérationnelles
Portage III 12C1 - 42
11 Laurier Street/11, rue Laurier
Gatineau
Quebec
K1A 0S5

Canada

INVITATION TO QUALIFY (ITQ)

FOR

ePassport Solution – Development, Production and Personalization Delivery Services for Immigration, Refugees and Citizenship Canada (IRCC)

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

1.1.1 This Invitation to Qualify (ITQ) is neither a Request for Proposal (RFP) nor a solicitation of bids or tenders. No Contract will result from this ITQ. Given that this ITQ may be cancelled by Canada, it may not result in any of the subsequent procurement processes described in this document. Suppliers are welcome to withdraw from the process at any time, as the ITQ is not a tender.

1.1.2 This ITQ is the first phase in the procurement process for the ePassport Solution. The objective of this ITQ is only to qualify responsive Suppliers to proceed to the subsequent phases of this procurement process. The responsive Suppliers will be hereinafter referred to as "Qualified Suppliers".

1.1.3 Only Qualified Suppliers will be permitted to receive draft RFP requirements.

1.1.4 Qualified Suppliers may choose not to bid on the final RFP.

1.1.5 This ITQ may be cancelled if less than 3 responses are received or if less than three (3) Suppliers are qualified. The ITQ may also be cancelled at any time in accordance with the 2003 (2017-04-27) Standard Instructions - Goods or Services – Competitive Requirements.

1.1.6 The ITQ is divided into the following parts:

Part 1: General Information: provides an overview of the ePassport Solution requirements;

Part 2: Supplier Instructions: provides the instructions, clauses and conditions applicable to the ITQ;

Part 3: Response Preparation Instructions: provides Suppliers with instructions on how to prepare their response to the ITQ;

Part 4: Overview of the Procurement Process;

Part 5: Evaluation Procedures and Basis of Qualification: describes how the responses will be evaluated and the basis of Qualification;

Part 6: Certifications: includes the certifications to be provided as part of the ITQ response;

Part 7: Security Requirement: describes specific security requirements;

Part 8: ITQ Process Terms of Engagement: sets out the terms governing the appropriate conduct of Suppliers; and

Part 9: Subset of Anticipated Resulting Contract Clauses: includes some anticipated clauses for the resulting Contract.

Refer to the Table of Contents for the list of annexes, attachments and forms.

1.2 Summary

1.2.1 Canada would like to enhance the security features of the current suite of Travel Documents and will be initiating a procurement process for the design and printing of new secure passport books for issuance in approximately four (4) years. The delivery of a secure ePassport that will reduce the risk of tampering and identity fraud is a key component of Canada's mandate. By having stronger features to support identity and other checks, secure ePassports reduce the risk of other countries putting visa requirements on travelers. Canada has selected a laser-engraved polycarbonate data page personalization process.

1.2.2 Canada has identified the following as components required for the production of the next generation ePassport:

1.2.2.1 Passport books incorporating an ePassport chip (i.e. contactless integrated circuit);
1.2.2.2 Public Key Infrastructure (PKI) environment (Certificate Authority, Document Signer, Certificate Revocation Lists, Master List signers, Active Authentication key pairs, other sub-Certificate Authorities and signers as required (e.g. visa signers), Links to International Civil Aviation Organization Public Key Directory (ICAO PKD));
1.2.2.3 Supplemental Access Control (SAC) and Logical Data Structure (LDS) v1.8;
1.2.2.4 Personalization of passport books by laser-engraving a polycarbonate data page where the ePassport chip is integrated inside the data page;
1.2.2.5 Encoding solution;
1.2.2.6 Interfaces between the different components of the solution;
1.2.2.7 Quality assurance and quality control equipment and/or services for personalized books;
1.2.2.8 Maintenance and Support Plan; and
1.2.2.9 Passport book design.

1.2.3 The purpose of this ITQ is to invite all Suppliers capable of meeting the requirements of this ITQ to submit responses to Public Works and Government Services Canada (PWGSC) for evaluation in an attempt to become a Qualified Supplier. Only Qualified Suppliers will be invited to participate in the draft RFP process.

1.3 Procurement Overview

1.3.1 The ePassport Solution procurement will be fulfilled through a multi-phased collaborative procurement process.

1.3.2 **ITQ:** This ITQ is open to all Suppliers and will result in Qualified Suppliers being invited to participate in the draft RFP process. Respondents will be notified of the evaluation results once the ITQ evaluation process is completed.

1.3.3 **Draft RFP**: A draft RFP will be issued to Qualified Suppliers to further refine the requirement by addressing industry concerns and considering industry best practices.

1.3.4 **Final RFP:** The RFP will be issued directly to Qualified Suppliers. Reference Part 8 for further details of the final RFP.

1.4 Debriefings (ITQ)

1.4.1 Suppliers may request a debriefing on the results of the ITQ. Suppliers should make the request to the Contracting Authority within 15 working days of receipt of the results of the ITQ.

1.5 Conflict of Interest

1.5.1 Suppliers are advised to refer to Conflict of Interest provisions at Article 18 of the Standard Acquisition Clauses and Conditions (SACC) 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2017-04-27) and Conflict of Interest provisions of SACC 2030, General Condition – Higher Complexity – Goods (dated 2016-04-04) available on the PWGSC Website **https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual**

1.5.2 Without limiting in any way the provisions described in 1.5.1 above, Suppliers are advised that Canada has engaged the assistance of the following private sector contractors and resources who have provided services including the preparation of this ITQ and/or who have had, or may have had, access to information related to this ITQ or other documents related to the ePassport Solution solicitation:

- Greg Thompson, Altis;
- Michael Bradshaw, Altis;
- Jean Montplaisir, Fairness Monitor, Public Sector Company;
- Bruce Maynard, Fairness Monitor, Public Sector Company; and
- Peter Woods, Fairness Monitor, Public Sector Company.

1.6 Fairness Monitor

1.6.1 Canada has engaged the services of an organization to act as an independent third party Fairness Monitor (FM) for the ePassport Solution procurement process. The role of the FM is to provide an attestation of assurance on the fairness, openness and transparency of the monitored activities.

1.6.2 The Fairness Monitor will not be part of the evaluation team, but will be granted access to any response submitted in response to this ITQ and any related correspondence received by Canada pursuant to this ITQ. The FM will observe the evaluation of the ITQ responses with respect to Canada's adherence to the evaluation process described in this ITQ and will observe the response debriefings.

1.7 Trade Agreements

1.7.1 This procurement is subject to national security exception and is, therefore, excluded from all of the obligations of the trade agreements.

PART 2 – SUPPLIER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 All instructions, clauses and conditions identified in the ITQ by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual)* issued by PWGSC.

2.1.2 Suppliers who submit a response agree to be bound by the instructions, clauses and conditions of the ITQ.

2.1.3 The 2003 (2017-04-27) Standard Instructions - Goods or Services – Competitive Requirements, are incorporated by reference into and form part of the ITQ, except that:

a. Wherever the term "bid solicitation" is used, it is substituted with "Invitation to Qualify";
b. Wherever the term "bid" is used, it is substituted with "response";
c. Wherever the term "Bidder(s)" is used, it is substituted with "Supplier(s)";
d. Wherever the terms "Contract (contract)" is used, it is substituted with "Qualification" or "Qualified Supplier" as applicable;
e. Subsection 5(4), which discusses a validity period, does not apply, given that this ITQ invites Suppliers simply to qualify;
f. The title of Section 10 is amended to read "Legal Capacity and Ownership and Control Information", the first paragraph is numbered as 1 and the following is added:

2. The Supplier must provide, if requested by the Contracting Authority, the following information as well as any other requested information related to the ownership and control of the Supplier, its owners, its management and any related corporations and partnerships:

i. An organization chart for the Supplier showing all related corporations and partnerships;

ii. A list of all the Supplier's shareholders and/or partners, as applicable; if the Supplier is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner; and

iii. A list of all the Supplier's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Supplier is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner.

In the case of a joint venture Supplier, this information must be provided for each member of the joint venture. The Contracting Authority may also require that this information be provided in respect of any Subcontractors specified in a response.

3. For the purposes of this section, a corporation or partnership will be considered related to another party if:

   i. they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act*;

   ii. the entities have now or in the two (2) years before the closing date had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

   iii. the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

g. Subsection 14 Price Justification does not apply as there is no financial component to the ITQ.

2.2 Composition of Core Team

2.2.1 Suppliers submitting responses to the ITQ must indicate the relevant company and/ or organization names (including Core Team Members) that are jointly submitting the response in Form 1: ITQ Submission Form.

2.2.2 If a response is submitted by a joint venture, it must be in accordance with section 17 Joint Venture, of the SACC 2003 Standard Instructions (2017-04-27).

2.2.3 Only the capabilities and experience of the Core Team will be considered when evaluating the response submitted to this ITQ.

2.2.4 The Core Team may be comprised of a Supplier and any additional firms deemed necessary by the Supplier (Core Team Members). The structure can either be prime (Supplier) and Subcontractors or a joint venture of two (2) or more of the members identified as the Core Team, if applicable.

2.2.5 Once a Supplier has identified itself as the Supplier, it must remain the Supplier and cannot switch roles with any member of its Core Team for the duration of the ePassport Solution procurement process. For Suppliers who qualify to proceed to the next phase of the procurement process, the Supplier must be the Bidder for the RFP.

2.2.6 A Supplier's Core Team for subsequent phases of the ePassport Solution procurement process must continue to consist of the Core Team identified in the response to this ITQ (Form 1). Beyond this period, changes to the Core Team may only be made following receipt of written approval from the Contracting Authority. Failure to maintain the Core Team throughout the procurement process (unless approved in writing by the Contracting Authority) may, at the discretion of Canada, result in the Supplier becoming ineligible for continued participation in the ePassport Solution procurement process.

2.2.7 Suppliers must, in their ITQ Response, identify what role each member of their Core Team will play in delivery of the ePassport Solution services. Further, the Supplier must demonstrate that where a Core Team member's experience has been proposed to meet Qualifications listed in the Mandatory Requirements section of the ITQ, that Core Team member will carry out the same work under any resulting Contract. For example, where a Supplier has identified itself as the Core Team member with the experience required for Mandatory Requirement 1 (M1), the Supplier will deliver that service under any resulting Contract.

2.3 Submission of Responses

2.3.1 Responses must be submitted only to the PWGSC Bid Receiving Unit by the date, time and place indicated on page 1 of the ITQ.

2.3.2 Due to the nature of the ITQ, transmission of responses by facsimile or e-mail to PWGSC will not be accepted.

2.4 Enquiries

2.4.1 All enquiries must be submitted in writing to the Contracting Authority, at the email address identified below, no later than 10 business days before the ITQ closing date. Enquiries received after that time may not be answered.

Michael Hradecky

Contracting Authority – ePassport Solution
Public Services and Procurement Canada

Email address: Michael.hradecky@tpsgc-pwgsc.gc.ca

2.4.2 Suppliers should reference as accurately as possible the numbered item of the ITQ to which the enquiry relates. Care should be taken by Suppliers to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. 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 question(s) or may request that Suppliers do so, so that the proprietary nature of the question(s) is eliminated,

and the enquiry can be answered to all Suppliers. Enquiries not submitted in a form that can be distributed to all Suppliers may not be answered by Canada.

2.5 Applicable Laws

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

2.6 Improvement of Requirement during ITQ

2.6.1 Should Suppliers consider that the requirements contained in the ITQ could be improved technically or technologically, Suppliers are invited to make suggestions, in writing, to the Contracting Authority named in the ITQ. Suppliers must clearly outline the suggested improvement as well as the reason for the suggestion. Only suggestions that do not restrict the level of competition nor favour a particular Supplier may be given consideration provided they are submitted to the Contracting Authority at least 10 working days before the ITQ closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Language

2.7.1 Suppliers are requested to identify, in writing, in Form 1 - ITQ Submission Form which of Canada's two (2) official languages (English or French) will be used for future communications from Canada and, if successful in the ITQ evaluation, for the draft RFP process.

2.8 Basis for Canada's Ownership of Intellectual Property

2.8.1 Canada has determined that any intellectual property arising from the performance of the Work under the Contract will belong to Canada, on the grounds of National Security.

Canada will own the intellectual property rights of the foreground to the ePassport book, the public key infrastructure solution, software/hardware solutions for all customized modules, custom Canadian consumables design and artwork, plates, dies and other custom tooling bearing Canadian designs used in the performance of work under the Contract. All other intellectual property rights, including background and other foreground, will be owned or licensed by the Contractor with appropriate licenses granted to Canada.

PART 3 - RESPONSE PREPARATION INSTRUCTIONS

3.1 Response Preparation Instructions

Canada requests that Suppliers provide their response in separate sections as follows:

Section I: Technical Response (One (1) master soft copy and two (2) additional soft copies on two (2) separate USB(s) in a format accessible by Canada). If there is a discrepancy between the wording of the master copy and any other copy, the wording of the master will have priority.

Section II: Certifications (One (1) master soft copy and One (1) additional soft copy on a USB in a format accessible by Canada).

Formats of electronic documents accessible by Canada include PDF or MS Office 2013.

Section I: Technical Response

In the technical response, Suppliers are requested to explain and demonstrate how their response meets the ITQ technical requirements.

The Technical Response must include submission of:

1. Form 1: ITQ Submission Form;
2. Attachment 1 to Part 5: Mandatory Evaluation Criteria; and
3. Form 2: Project Reference Check Form.

Section II: Certifications

Suppliers must submit the certifications required under Part 6.

PART 4 - OVERVIEW OF PROCUREMENT PROCESS

4.1 Overview

4.1.1 The Qualification Phase is the first phase of the ePassport Solution multi-phase procurement process as shown in Figure 1 and summarized in Table 1. Additional Information on the ePassport Solution procurement process can be found in Annex 2: Draft ePassport Solution Procurement Process - Post Qualification Phase to this ITQ.

4.1.2 The ITQ defines the requirements for the Qualification Phase. The objective of the Qualification Phase is to qualify Suppliers for further consideration in the ePassport Solution procurement process. Refer to Part 5 of the ITQ for a more detailed explanation of the ITQ Evaluation Procedures and Selection of Qualified Suppliers.

Figure 1. ePassport Solution Procurement Approach

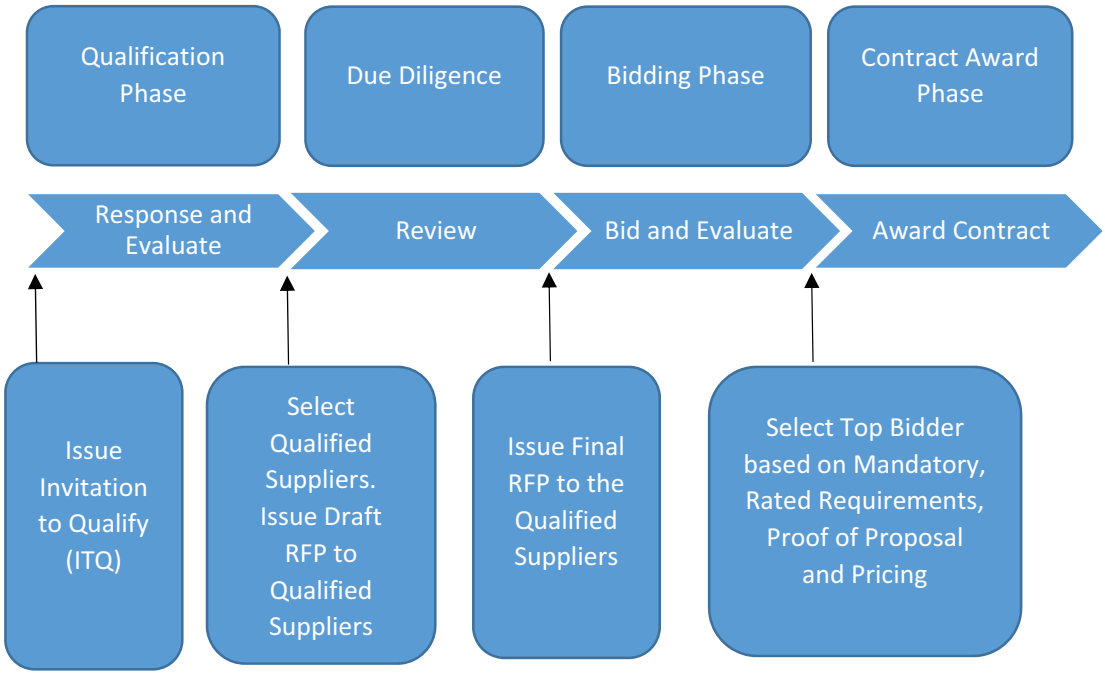


Table 1: Summary of ePassport Solution Procurement Phases and Objectives

Procurement Phase	**Objectives**
Qualification	• Issue ITQ on *Buyandsell.gc.ca* • Obtain ITQ responses from Suppliers • Evaluate ITQ responses • Select the Qualified Suppliers that will move on to the Due Diligence phase
Due Diligence	• Provide the Qualified Suppliers with a draft of the ePassport Solution RFP • Provide the Qualified Suppliers an opportunity to enhance their understanding of the ePassport Solution requirements • Provide Canada with an opportunity to obtain recommendations for improvements to the ePassport Solution requirements from Qualified Suppliers • Canada may modify ePassport Solution requirements to incorporate changes approved by Canada
Bidding	• Issue RFP to all Qualified Suppliers • Obtain complete bids from the Bidders • Evaluate and rank the bids
Contract Award	• Award the ePassport Solution Contract to the winning Bidder

PART 5 - EVALUATION PROCEDURES AND BASIS OF QUALIFICATION

5.1 Evaluation Procedures

5.1.1 Responses will be assessed in accordance with the entire requirement of the ITQ including the technical evaluation criteria.

5.1.2 An evaluation team composed of representatives of Canada and possibly independent consultants will evaluate the responses. Canada may hire any independent consultant, consulting firm or use any Government resources to evaluate any ITQ response. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation. By submitting a response, Suppliers consent to the release of those responses to the third-party consultants retained by Canada, subject to Canada's obtaining confidentiality undertakings from these third-party consultants.

5.1.3 In addition to any other time periods established in the solicitation process:

a. Requests for Clarifications: If Canada seeks clarification or verification from the Supplier about its response, the Supplier will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada; and

b. Extension of Time: If additional time is required by the Supplier, the Contracting Authority may grant an extension at his or her sole discretion.

5.2 Technical Evaluation

5.2.1 Each response will be reviewed for compliance with the mandatory requirements of this ITQ. Responses that do not comply with each and every mandatory requirement will be considered non-responsive and given no further consideration.

5.2.2 The Mandatory Evaluation Criteria, and Substantiation of Technical Compliance - Mandatory Evaluation Criteria, are described in Attachment 1 to Part 5.

5.2.3 Suppliers should demonstrate their understanding of the requirements contained in this ITQ and address clearly and in sufficient depth the points that are subject to the evaluation. Simply repeating the statement contained in the ITQ is not sufficient.

5.2.4 In conducting its evaluation of the responses, Canada may, but will have no obligation to, do the following:

a. contact any or all references supplied by Suppliers to verify and validate any information submitted by the Suppliers; and
b. seek clarification or verification from Suppliers regarding any or all information provided by them with respect to the ITQ.

5.2.5 Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given mandatory requirement, it will check the references for that requirement for all Suppliers who have not, at that point, been found non-responsive.

5.2.6 Only referenced material included within the Supplier's response, or clarified upon request by the Contracting Authority, will be evaluated. Reference material outside of the Supplier's response will not be considered. It is the sole responsibility of the Supplier to provide sufficient information so that their responses can be adequately evaluated.

5.3 Reference Checks

5.3.1 The Supplier is requested to provide a third-party reference for each project in its response as requested in Attachment 1 to Part 5: Mandatory Evaluation Criteria, using Form 2: Project Reference Check Form. If information requested is not provided in the response, the Supplier must provide the information upon request by the Contracting Authority within the timeframe identified in the request. References from representatives of Canada will be accepted.

5.3.2 It is the responsibility of the Supplier to confirm in advance that their client contact for the project reference will be available to provide a response and is willing to provide a reference.

5.3.3 For the purpose of this evaluation, reference checks may be used to verify and validate the Supplier's response. If a reference check is performed, Canada will conduct the reference check in writing by e-mail. Canada will send the reference check request directly to the client contact for the project reference provided by the Supplier. The client contact will have 5 working days (or a longer period otherwise specified in writing by the Contracting Authority) from the date that Canada's e-mail was sent, to respond to Canada.

5.3.4 The client contact will be required, within 2 working days after Canada sends out the reference check request, to acknowledge the receipt of the reference check request and identify his or her willingness and availability to conduct such reference check. If Canada has not received the required response from the client contact, Canada will notify the Supplier by e-mail, to allow the Supplier to contact its client contact directly to ensure that he or she responds to Canada within the allotted time. The client contact's failure to respond to Canada's request in a timely manner will result in non-consideration of the Supplier's claimed project experience.

5.3.5 Notwithstanding section 5.3.3, if the client contact is unavailable when required during the evaluation period, the Suppliers will be requested to provide an alternate client contact for the same referenced project. Suppliers will only be provided with this opportunity once for each referenced project and only if the original client contact is unavailable to respond. The process as described in 5.3.3 is applicable for the reference check with the alternate client contact. The period to respond for either the original client

contact, or the alternate client contact, will be a total of 5 working days (or a longer period otherwise specified in writing by the Contracting Authority) in accordance with 5.3.3.

5.3.6 Wherever information provided by a client contact differs from the information supplied by the Supplier, the Supplier will be asked to clarify project reference information provided in its ITQ response. Canada will assess the following information during the evaluation of the Supplier's response: the Supplier's original project reference information; any information provided by the Supplier in response to clarification request(s); and any information supplied by the client contact for the referenced project.

5.3.7 A Supplier will not meet the mandatory experience requirement if:
(1) the client contact fails to respond to Canada's request in a timely manner;
(2) the client contact states he or she is unable or unwilling to provide the information requested;
(3) the information provided by the Supplier cannot be verified and validated by Canada; or
(4) the client is itself an affiliate or other entity that does not deal at arm's length with the Supplier.

5.4 Basis of Qualification

5.4.1 **Selection of Qualified Suppliers**

5.4.1.1 To be declared responsive, a response must:

a. comply with all the requirements of this ITQ; and
b. comply with all of the Mandatory Evaluation Criteria (Attachment 1 to Part 5).

Otherwise, a response will be declared non-responsive and given no further consideration.

5.4.1.2 Respondents whose responses are deemed responsive will be selected as Qualified Suppliers to participate in the draft RFP process.

PART 6 – CERTIFICATIONS

Respondents must provide the required certifications and associated information to become a Qualified Supplier.

The certifications provided by Suppliers to Canada are subject to verification by Canada at all times. Canada will declare a response non-responsive, if any certification made by the Respondent is found to be untrue whether made knowingly or unknowingly during the ITQ response evaluation period.

The Contracting Authority will have the right to ask for additional information to verify the Respondent's certifications. Canada has the right to terminate the Respondent status, if the Respondent fails to comply and to cooperate with any request or requirement imposed by the Contracting Authority.

6.1 Certifications Precedent to becoming a Qualified Supplier

The certifications listed below should be completed and submitted with the response, but may be submitted afterwards. If any of these required certifications are not completed and submitted as requested, the Contracting Authority will inform the Respondent and provide it with a time frame within which to provide the information. Failure to comply with the request of the Contracting Authority and to provide the certifications within the time frame will render the response non-responsive.

6.1.1 Integrity Provisions – Required Documentation

In accordance with the Ineligibility and Suspension Policy *(*http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Respondent must provide the required documentation, as applicable, to be given further consideration in the procurement process.

6.1.2 Former Public Servant – Competitive Response

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on Contracts awarded to FPSs, Respondents must provide the information required below before Contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of responses is completed, Canada will inform the Respondents of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

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

a. an individual;

b. an individual who has incorporated;

c. a partnership made of former public servants; or

d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

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

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

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Respondent a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Respondent must provide the following information, for all FPSs in receipt of a pension, as applicable:

a. name of former public servant;

b. date of termination of employment or retirement from the Public Service.

By providing this information, Respondents agree that the successful Respondent's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with

Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

Is the Respondent a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Respondent must provide the following information:

a. name of former public servant;

b. conditions of the lump sum payment incentive;

c. date of termination of employment;

d. amount of lump sum payment;

e. rate of pay on which lump sum payment is based;

f. period of lump sum payment including start date, end date and number of weeks;

g. number and amount (professional fees) of other Contracts subject to the restrictions of a work force adjustment program.

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

6.1.3 Acknowledgement

By submitting a response, the Supplier represents that it has full authority to bind the company and individuals representing the company, to be bound by all the terms and conditions contained herein.

PART 7 - SECURITY REQUIREMENT

7.1 Security Requirement

7.1.1 There are no security requirements for the ITQ.

7.1.2 There will be security requirements for the RFP. Preliminary security requirements for the RFP and resulting Contract are outlined in Part 9 of this document to assist Suppliers in preparing for the RFP security requirements.

7.1.3 As there will be security requirements for the RFP and resulting Contract, Suppliers that do not currently have personnel and organization security clearances through the Canadian federal government or their respective domestic Industrial Security Program, or Suppliers that do not meet the anticipated security requirements outlined in Part 9, should begin the clearance process early by contacting the Industrial Security Program (ISP) of PWGSC (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website, or their respective domestic Industrial Security Program, as applicable.

PART 8 - ANTICIPATED RFP

8.1 Bid Solicitation Components

8.1.1 Canada will use the High Complexity (HC) bid solicitation template for the anticipated RFP.

8.1.2 A copy of the template can be provided upon request by contacting the Procurement Process Tools Division by sending a query to Outilsd'approvisionnement.ProcurementTools@tpsgc-pwgsc.gc.ca.

8.1.3 The latest versions of the template and terms and conditions will be used in the anticipated RFP. The numbering of sections, annexes, attachments and forms may change in the final RFP.

8.1.4 At a minimum the anticipated RFP may contain the following:

a. security, database location, and privacy requirements;
b. financial capability (reference SACC A9033T);
c. a complete description of the Work to be performed;
d. 2003, Standard Instructions - Goods or Services - Competitive Requirements;
e. bid preparation instructions;
f. instructions for the submission of bids;
g. evaluation procedures and basis of selection;
h. terms and conditions of the resulting Contract; and
i. certifications.

8.1.5 It is anticipated that certifications, at time of bid submission, may include, but may not be limited to the following:
1) Integrity Provisions - Associated Information;
2) Former Public Servant – Competitive Bid (reference SACC A3025T);
3) Federal Contractors Program for Employment Equity – Bid Certification; and
4) Status and Availability of Subcontractors Providing Core Services.

PART 9 - SUBSET OF ANTICIPATED RESULTING CONTRACT CLAUSES

9.1 General

9.1.1 The conditions of any Contract awarded as a result of the RFP will be in accordance with the relevant resulting Contract clauses of the HC template used for the RFP.

9.1.2 Only a subset of the anticipated resulting Contract clauses are included in this section in order to provide Suppliers advance notice, as well as to allow Suppliers time to consider the impact of said clauses and provide feedback to Canada as required.

9.2 Standard Clauses and Conditions

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

9.2.1 General Conditions

2030 (2016-04-04), General Conditions – Higher Complexity – Goods, apply to and form part of the Contract.

9.3 Anticipated Security Requirements

Only a subset of the anticipated RFP security clearance requirements are included in this section in order to provide Suppliers advance notice of said requirements. It is anticipated the security clearance requirements will be expanded in the RFP. It is also anticipated that the personnel and facility(ies) proposed by the Supplier in the design, manufacture and storage of the Canadian travel documents must hold the required security clearances at the closing date of the RFP.

For information purposes, Suppliers are hereby informed that the amount of time to obtain required security clearance levels may be lengthy and is contingent upon the specific clearance levels required. Suppliers are solely responsible for obtaining such clearances.

A. Anticipated Security Requirement for Canadian Suppliers:

1. The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level **of SECRET with approved Document Safeguarding and Production Capabilities at the level of SECRET**, issued by the Canadian Industrial Security Directorate (CISD), 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 personnel requiring access to **CLASSIFIED** information, assets or sensitive work site(s) must **EACH** hold a valid personnel security screening at the level of **SECRET**, granted or approved by the CISD/PWGSC.

4. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store any sensitive **PROTECTED** information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of **PROTECTED B, including an IT Link at the level of PROTECTED B.**

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

6. The Contractor must comply with the provisions of the:

   (a) Security Requirements Check List and security guide, attached at Annex 5: Security Requirement Checklist (SRCL); and
   (b) Industrial Security Manual (Latest Edition).

B. Anticipated Security Requirement for International Suppliers:

The Contractor and/or any and all Subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website:

http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html

All **CANADA PROTECTED / CLASSIFIED SECRET** information/assets, furnished to the Foreign recipient **Contractor / Subcontractor** or produced by the Foreign recipient **Contractor / Subcontractor**, shall be safeguarded as follows:

1. The Foreign recipient **Contractor / Subcontractor** shall, at all times during the performance of the **Contract / Subcontract**, hold a valid Facility Security Clearance, issued by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the suppliers country,** at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET** and an authorization to produce (manufacture, and/or repair, and/or modify or otherwise work on) material or equipment at the Foreign recipient **Contractor / Subcontractor** sites, at the level of **SECRET**, issued by the NSA or DSA for industrial security of **the Suppliers country** in accordance with the national policies of **the Suppliers country**.

2. All **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated under this **Contract / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Subcontract**, in accordance with the national policies of **the Suppliers country.**

3. The Foreign recipient **Contractor / Subcontractor** shall provide the **CANADA PROTECTED / CLASSIFIED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the national policies, National Security legislation and regulations and as prescribed by the NSA or DSA of **the Suppliers country**.

4. All **CANADA PROTECTED / CLASSIFIED** information/assets provided to the Foreign recipient **Contractor / Subcontractor** pursuant to this **Contract / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor /Subcontractor** with the equivalent security classification utilized by **the Suppliers country** and in accordance with the national policies of **the Suppliers country**.

5. The Foreign recipient **Contractor / Subcontractor** shall, at all times during the performance of this **Contract / Subcontract**, ensure the transfer of **CANADA PROTECTED / CLASSIFIED** information/assets be facilitated in accordance with the national policies of **the Suppliers country**, and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the Suppliers country** and Canada.

6. Upon completion of the work, the Foreign recipient **Contractor / Subcontractor** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED / CLASSIFIED** information/assets furnished or produced pursuant to this **Contract / Subcontract**, including all **CANADA PROTECTED / CLASSIFIED** information/assets released to and/or produced by its Subcontractors.

7. **CANADA CLASSIFIED / PROTECTED** information/assets shall be released only to Foreign recipient **Contractor / Subcontractor** personnel, who have a need-to-know for the performance of the **Contract / Subcontract** and who have a Personnel Security Clearance at the level of **SECRET**, as required, granted by their respective NSA or DSA of **the Suppliers country**, in accordance with national policies of **the Suppliers country**.

8. **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated pursuant to this **Contract / Subcontract** shall not be further provided to a third party Foreign recipient Subcontractor unless:
   a. written assurance is obtained from the third-party Foreign recipient's NSA or DSA to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **CANADA PROTECTED / CLASSIFIED** information by the third-party Foreign recipient's NSA/DSA; and
   b. written consent is obtained from the NSA/DSA of **the Suppliers country**, if the third-party Foreign recipient Subcontractor is located in a third country.

9. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of their respective NSA or DSA, in accordance with the national policies of **the Suppliers country.**

10. The Foreign recipient **Contractor / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED** information until the NSA or DSA of **the Suppliers country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Subcontractor**, these tasks may be performed up to the level of **PROTECTED B.**

11. The Foreign recipient **Contractor / Subcontractor** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Contract / Subcontract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

12. The Foreign recipient **Contractor / Subcontractor** visiting Canadian Government or industrial facilities, under this contract, will submit a Request for Visit form to Canada's DSA through their respective NSA or DSA.

13. The Foreign recipient **Contractor / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA CLASSIFIED / PROTECTED** information / assets pursuant to this **Contract / Subcontract** has been compromised.

14. The Foreign recipient **Contractor / Subcontractor** shall immediately report to its respective NSA or DSA all cases in which it is known or there is reason to suspect that **CANADA CLASSIFIED / PROTECTED** information/assets accessed by the Foreign recipient **Contractor / Subcontractor**, pursuant this **Contract / Subcontract**, have been lost or disclosed to unauthorized persons.

15. The Foreign recipient **Contractor / Subcontractor** shall not disclose the **CANADA CLASSIFIED / PROTECTED** information to a third party government, person, firm or representative thereof, without the prior written consent of the GOC. Such consent shall be sought through the recipient's NSA/DSA.

16. The Foreign recipient **Contractor / Subcontractor** shall comply with the provisions of the International bilateral industrial security instrument between **the Suppliers country** and Canada, in relation to equivalencies.

17. The Foreign recipient **Contractor / Subcontractor** must comply with the provisions of the SRCL and security guide, attached at Annex 5: Security Requirement Checklist.

18. In the event that a Foreign recipient **Contractor / Subcontractor** is chosen as a supplier for this Contract, subsequent Country-Specific Foreign security requirement clauses shall be generated and promulgated by the Canadian DSA, and provided to the GOC Contracting

Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

ANNEXES

ANNEX 1: HIGH LEVEL REQUIREMENTS

1.0 EPASSPORT SOLUTION BACKGROUND

The Government of Canada (GOC) has been issuing electronic machine-readable passports (ePassports) through the Passport Program of Citizenship and Immigration Canada (CIC) since February 4, 2013. The current passport contains a number of features:

(a) Custom artistic design;
(b) Custom paper substrate including a watermark and inclusions;
(c) Secure printing (offset, UV, IR, Intaglio, OVI, letterpress, registered features, etc.);
(d) Quality cover material, hot foil stamping and an ultraviolet multi-color sewing thread;
(e) Dye-based Inkjet personalization;
(f) Secure holographic laminate; and
(g) ICAO Doc 9303 Part 9 compliant contactless integrated circuit.

The data page of the ePassport is personalized at Passport Program print sites. The ePassport chip contains the same data elements that are found in the Machine Readable Zone (MRZ), the facial image of the holder, and information that, when verified by an inspection system, proves that the chip is not a clone. The information on the chip is protected with a digital signature that can be used to confirm that the chip is authentic and that the data has not been tampered with. The personal information stored on the ePassport chip is privacy protected by Basic Access Control (BAC).

Canada has determined the preferred options for the production, and planned implementation in fiscal year 2020-2021, of a highly secure passport manufactured in accordance with technical specifications (Doc 9303) published by the ICAO.

The current ePassport Contract will therefore be replaced by a new contractual instrument to provide Canada with a Next Generation ePassport solution that will be focused on the production process and will provide the best combination of service to Canadian citizens.

2.0 CURRENT ePASSPORT PRODUCTION

Canada currently uses two (2) Print Centres for personalizing about 86% of the volume of ePassports issued using high-volume printers. The remaining 14% are printed locally in the Regional Offices. There is an ePassport reader in each office. See chart below for a representative overview of Canada's decentralized printing model.

Print Centres	High-volume printers	ePassport reader
Gatineau **(Size of print room: 1128 pi^2 / 104.8 m^2)**	2 working units (+ 3 back-up)	2 working units (+ 3 back-up)
Mississauga **(Size of print room: 1017 pi^2/ 96.5 m^2)**	2 working units (+ 2 back-up)	2 working units (+ 2 back-up)

Regional Offices	Regional printers	ePassport readers
Calgary	2	2
Edmonton	1 (+1)*	1 (+1)*
Regina	1 (+1)*	1 (+1)*
Saskatoon	1 (+1)*	1 (+1)*
Surrey	1 (+1)*	1 (+1)*
Vancouver	2	2
Victoria	1 (+1)*	1 (+1)*
Winnipeg	1 (+1)*	1 (+1)*
Calgary South	0	0
Kelowna	0	0
Richmond	0	0
Hamilton	1	1
Kitchener	1	1
London	2	2
Mississauga	2	2
North York	2	2
Scarborough	2	2
St. Catharines	1	1
Thunder Bay	1 (+1)*	1 (+1)*

Toronto	2	2
Windsor	1 (+1)*	1 (+1)*
Brampton	0	0
Whitby	0	0
Fredericton	1 (+1)*	1 (+1)*
Gatineau	2	2
Halifax	1 (+1)*	1 (+1)*
Laval	2	2
Montreal	2	2
Ottawa	1	1
Québec	1 (+1)*	1 (+1)*
Saguenay	1 (+1)*	1 (+1)*
St. John's	1 (+1)*	1 (+1)*
Saint-Laurent	2	2
Pointe-Claire	0	0

*: + 1 back-up on site but not in use

Note: These numbers are representative, not actual and are subject to change.

3.0 HIGH-LEVEL NEXT GENERATION EPASSPORT SOLUTION REQUIREMENT

Canada would like to enhance the security features of the suite of Travel Documents and is initiating the process to be able to design and be ready to print new secure passport books in approximately four (4) years. The delivery of a secure ePassport that will reduce the risk of tampering and identity fraud is a key component of Canada's mandate. By having stronger features to support identity and other checks, secure ePassports reduce the risk of other countries putting visa requirements on Canadian travelers. Canada has selected a laser-engraved polycarbonate data page personalization process,

Canada will not consider dye diffusion thermal transfer, dye sublimation, toner, all pigment or dye based inkjet, UV curable inkjet or other personalization technologies.

This is projected to be a complex, multi-year requirement composed of closely linked components. Future procurement actions may result in the award of one (1) Contract with an initial contract period of seven (7) years with an option to extend the period of the Contract by up to seven (7) additional one (1) year periods.

Canada has identified the following as components required for the production of the next generation ePassport:

(a) Passport books incorporating an ePassport chip;

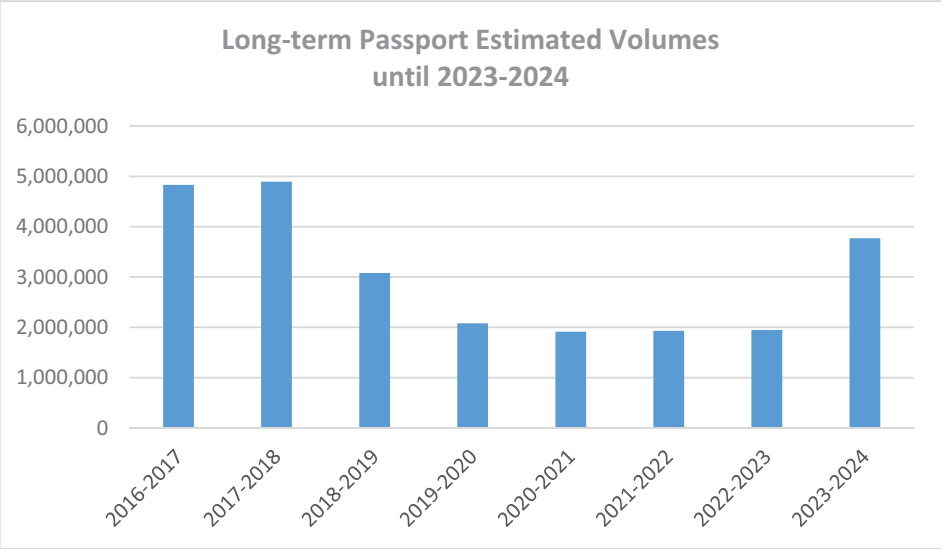
(b) PKI environment (Certificate Authority, Document Signers, Certificate Revocation Lists, Master List signers, Active Authentication key pairs, other sub-Certificate Authorities and signers as required (e.g. visa signers), Links to ICAO PKD);
(c) Supplemental Access Control (SAC) and Logical Data Structure (LDS) v1.8;
(d) Personalization of passport books by laser-engraving a polycarbonate data page where the ePassport chip is integrated inside the data page;
(e) Encoding solution;
(f) Interfaces between the different components of the solution;
(g) Quality assurance/quality control equipment and/or services for personalized books;
(h) Maintenance and support plan; and
(i) Passport book design.

Canada recognizes that certain materials, hardware and consumables required for an ePassport Solution may have to be sourced from outside Canada. Canada has determined that manufacturing, as defined in Annex 3, must occur in Canada.

4.0 ESTIMATED PASSPORT PRODUCTION VOLUMES

The charts below provide estimated volumes of expected ePassport production. The quantities are based on information available at the time of posting this ITQ and are not a guarantee that the same quantities will be produced under any future RFP and/or Contract. This data is for information purposes only.

Year	Estimated Volumes
2017-2018	5,248,765
2018-2019	3,245,879
2019-2020	2,077,734
2020-2021	1,913,308
2021-2022	1,930,702
2022-2023	1,944,759
2023-2024	3,769,325



Note: It is anticipated that estimated volumes will return to 5.5 million passports/year during the duration of the future contract although current forecasts do not extend beyond 2024.

5.0 HISTORICAL PASSPORT PRODUCTION VOLUMES

The charts below provides fiscal year totals of books personalized by the ePassport Program.

Year	Historical Volumes
2012-2013	5,041,245
2013-2014	4,806,750
2014-2015	5,033,759
2015-2016	4,712,722
2016-2017	4,870,683

ANNEX 2: DRAFT EPASSPORT SOLUTION PROCUREMENT PROCESS – POST QUALIFICATION PHASE

1. OVERVIEW

(a) The latest draft of the ePassport Solution procurement process is described in this annex. It will remain a draft until the final RFP is issued to the Qualified Suppliers. The ePassport Solution procurement approach will use a multi-phase process, as shown below. This approach will allow Canada to conduct due diligence of ePassport Solution requirements with Qualified Suppliers before issuing the bid solicitation. Because the post Qualification Phases of the ePassport Solution procurement may be very labour intensive and time consuming for both Suppliers and Canada, PWGSC will only be conducting this phase with the Qualified Suppliers as determined in the Qualification Phase. PWGSC's intention, in conducting the Due Diligence Phase prior to issuing the final bid solicitation, is to ensure that the Qualified Suppliers have an opportunity for a detailed review of the draft ePassport Solution solicitation prior to Canada distributing the Final RFP.

Step in Procurement Phase Components Process	**Phase**	**Components**
1. Issue ITQ	Qualification Phase	• Mandatory Requirements (Pass/Fail) • Select Qualified Suppliers
2. Distribute Draft RFP to Qualified Suppliers	Due Diligence	• Qualified Supplier review of Draft RFP and Security Profile Protection Table • Qualified Supplier recommendations and questions based on review of Draft RFP • Finalize RFP
3. Issue Final RFP to Qualified Suppliers	Bidding Phase	• Mandatory Requirements (Pass/Fail) • Rated Requirements (Score) • Proof of Proposal Demonstration (Score) • Financial (Score) • Select Winning Bidder
4. Issue Contract to Winning Bidder	Contract Award Phase	• Award Contract

(b) Once the Qualified Suppliers have been selected and have been notified that they have qualified for the next phase of the procurement process, Canada intends to proceed with the Due Diligence Phase and will forward an electronic copy of the draft ePassport Solution RFP to each Qualified Supplier.

(c) Qualified Suppliers may withdraw from the process by providing written notification to the Contracting Authority.

(d) At any point, Canada may, at its sole discretion (but with no obligation to do so) choose to extend the time period for any post Qualification phase of this procurement.

2. DUE DILIGENCE

(a) It is the responsibility of each of Qualified Supplier to take advantage of the Due Diligence process by asking any questions that are necessary for it to prepare a complete response to the final bid solicitation.

(b) The objectives of the Due Diligence Phase include:

(i) Ensuring that the Qualified Suppliers have an opportunity to conduct a thorough review of the draft ePassport Solution RFP;

(ii) Obtaining recommendations for improvements to ePassport Solution RFP which are advantageous for Canada; and

(iii) Modifying the draft ePassport Solution RFP to incorporate changes approved by Canada.

(c) The approach for the Due Diligence Phase is as follows:

(i) During the Due Diligence Phase, Qualified Suppliers will have 20 working days to submit questions on the draft ePassport Solution RFP. Canada will respond to the questions and provide copies of the responses to each Qualified Supplier. All questions and answers will be provided to all Qualified Suppliers.

(ii) Questions 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 question(s) or may request that Qualified Suppliers do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Qualified Suppliers. Questions not submitted in a form that can be distributed to all Suppliers may not be answered by Canada.

3. BIDDING PHASE

(a) The objectives of the Bidding Phase include:

(i) Issuing the Final ePassport Solution RFP to the Qualified Suppliers (now referred to as Bidders);

(ii) Obtaining the bids from the Bidders;

(iii) Evaluating the bids; and

(iv) Selecting the successful Bidder.

(b) The approach for the Bidding Phase is as follows:

(i) The RFP will include both mandatory and rated requirements. The rated requirements evaluation will include the rated requirements provided in the RFP and the details of a scripted Proof of Proposal (PoP) test.

(ii) The PoP test will be conducted at no cost to Canada, at a location in Canada proposed by the Bidder and agreed to by Canada. Canada will confirm the location of the PoP test at least 30 days in advance. Each responsive Bidder must perform the PoP test in accordance with a timeframe, schedule, and agenda defined by the Government of Canada (GOC). Bidders will be notified of the date, and time of their PoP test no later than 15 working days prior to the PoP test. The responsive Bidders will be responsible for ensuring that the location is equipped with all the equipment necessary to conduct the PoP.

(iii) The PoP test content will be based on the proposed ePassport Solution functionality testing and conformance to the proposed Technology Blueprint submitted in response to the RFP.

(iv) It is at the Bidder's discretion to determine the appropriate team members to participate in the PoP. It is recommended that the team members include:

(A) Program Executive: The Bidder’s senior executive with ongoing accountability and responsibility for the ePassport Solution program and the individual who represents the Supplier’s Chief Executive Officer in all matters;

(B) Program Manager: The Bidder’s senior manager with on-going operational responsibility for delivery of the ePassport Solution services; and

(C) Technical Architect: A senior technical representative who has responsibility for technical architecture and design of the ePassport Solution services.

(v) On the day of the PoP each Bidder must provide:

(A) softcopy and hardcopy of the presentation;

(B) softcopy and hardcopy of documentation that is required to support the Bidder’s presentation; and

(C) Client references that the Bidder is using to support the presentation, if applicable.

4. CONTRACTOR SELECTION

(a) The details of the Contractor Selection process will be provided in the ePassport Solution RFP.

(b) Canada has not yet finalized the Contractor Selection methodology for the final RFP but it is anticipated that the bids received from Qualified Suppliers in response to the final RFP will be evaluated on the basis of:

- Compliance with mandatory requirements / security profile protection table;
- Rated technical experience, with a minimum pass mark;
- Rated PoP demonstration (testing of solution performance, usability and conformance to technical bid); and
- Rated financial proposal.

After complying with mandatory requirements, the Technical Proposal, PoP demonstration and Financial Proposal will be scored separately.

ANNEX 3: GLOSSARY OF TERMS

Term	Definition
Access Control	Access control is a security mechanism used on the ePassport chip to protect the privacy of the holder by preventing unauthorized access to ePassport data and to prevent eavesdropping of the communication between a chip and a reader.
BAC	The Canadian ePassport currently uses Basic Access Control (BAC), which requires the inspection system attempting to open the ePassport chip to provide a password, derived from sections within the MRZ, before the reader is granted access to the data. To protect against eavesdropping, BAC encrypts the communication between the reader and the ePassport chip using secure messaging.
Blank	Adjective used to describe Travel Documents that have not been personalized with the passport holder's personal information. No information is therefore incorporated on page 2 of the Travel Document and no information is incorporated on the ePassport Chip.
Consumables	Materials that need to be continuously replenished. ePassport related consumables may include, but are not limited to, laminate, ink or similar materials used in personalizing Blank ePassports.
DOC 9303	The ICAO Document 9303, a document defining specifications for machine readable travel documents.
Electronic travel document	A Machine Readable Travel Document that is compliant with ICAO Doc 9303 parts 1, 2, 3 and 4 and that contains a contactless integrated circuit compliant with parts 9, 10, 11 and 12.
ePassport	All Machine Readable Travel Documents that are compliant with ICAO Doc 9303 parts 1, 2, 3 and 4 and that contain a contactless integrated circuit compliant with parts 9, 10, 11 and 12 (including Certificates of Identity and Refugee Travel Documents). The term ePassport does not include passport cards.
ePassport chip	Doc 9303 compliant contactless integrated circuit.
ePassport Personalization System	The personalization equipment, related hardware, software, consumables, and any other materials that are used in combination to personalize Blank ePassports.
ePassport Solution	Defined by a new book design, all blank Travel Documents and consumables, a Public Key Infrastructure Solution, an ePassport Personalization System, a personalization solution and a support and maintenance plan.
Logical Data Structure (LDS) version 1.8	The LDS refers to the manner in which data is stored on the ePassport chip; using this standardized structure ensures global interoperability. ICAO Doc 9303 defines all mandatory and optional data elements and a prescriptive ordering and/or grouping of these elements. With each new LDS version changes to data element mapping occurs; version 1.8 is the latest version.

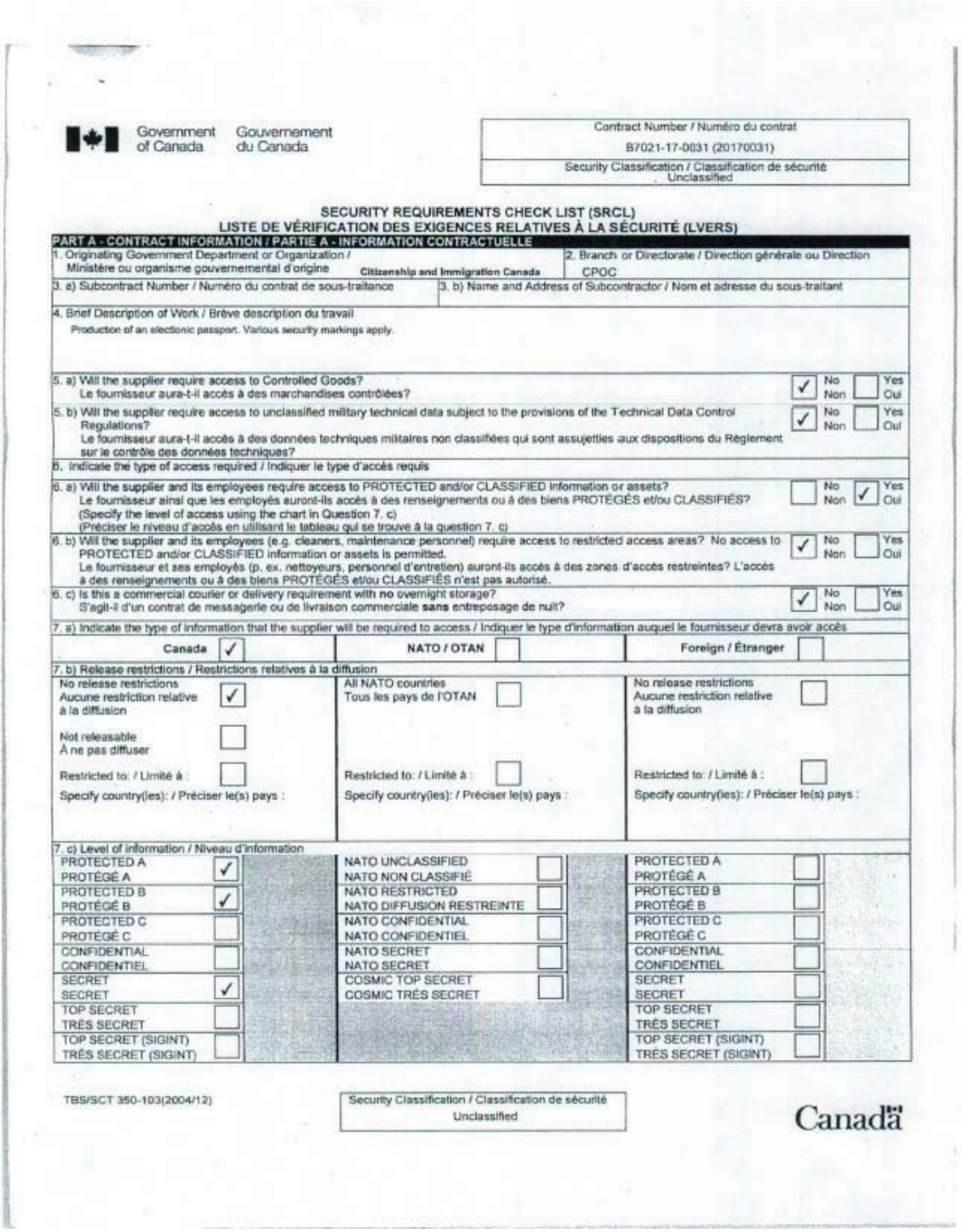
Low-Volume Printer	A low-volume printer is a lesser output counterpart to the high-volume printers. The low-volume configuration is scaled to suit a regional issuance model, while continuing to provide forensically identical personalization output
Machine Readable Travel Document (MRTD)	A Travel Document that is compliant with ICAO Doc 9303, specifically parts 1, 2, 3 and 4 and is issued by a State or organization for the purposes of international travel.
Manufacture or Manufacturing	The words "manufacture" or "manufacturing" of Blank ePassports or other Blank Travel Documents or components thereof used in this document refer, as a minimum, to the secure printing of all pages, the printing and lamination of the laser engraveable polycarbonate data page and the final assembly of such Travel Documents performed by the Contractor. Those steps must occur within the borders of Canada.
Password Authenticated Connection Establishment (PACE)	Access control is a security mechanism used on the ePassport chip to protect the privacy of the holder by preventing unauthorized access to ePassport data and to prevent eavesdropping of the communication between a chip and a reader. PACE improves upon the previous technology (i.e. BAC) by strengthening of the protection of the secure communication between the ePassport chip and readers/inspection systems.
Public Key Infrastructure (PKI) Solution	A set of policies, processes and technologies used to verify, enrol and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.
Passport Program Designated Locations	Locations in which the Passport Program, at its sole discretion, will require the installation of the ePassport Solution or components thereof.
Passport Program Issuance Engine	The internal Passport Program systems and processes that support the issuance of Travel Documents and maintain the personalization and reporting data required to administer and ensure the integrity of the issuance process.
Supplementary Access Control (SAC)	Access Control is a security mechanism used on the ePassport chip to protect the privacy of the holder by preventing unauthorized access to ePassport data and to prevent eavesdropping of the communication between a chip and a reader. SAC is a term used within the community to describe having both BAC and PACE on the ePassport chip. This is done to ensure backwards compatibility with inspection systems that are not yet updated to use PACE.
Travel Document	An identity document issued by a State for the purpose of international travel. The term Travel Document is used to represent all documents whether they are ePassports, MRTDs or not, that are eventually issued by Canada (including Temporary passports, Emergency Travel Documents, Certificates of Identity and Refugee Travel Documents). The term Travel Document does not include passport cards.

ANNEX 4: ACRONYMS

Acronym	Description
BAC	Basic Access Control
CIC	Citizenship and Immigration Canada
CISD	Canadian Industrial Security Directorate
CSP	Contract Security Program
DSA	Designated Security Authority
EU	European Union
GOC	Government of Canada
ICAO	International Civil Aviation Organization
IISD	International Industrial Security Directorate
ITQ	Invitation to Qualify
LDS	Logical data Structure
MRZ	Machine Readable Zone
NSA	National Security Authority
NATO	North Atlantic Treaty Organization
OCR-B	Optical Character Recognition- B
OVI	Optical Variable Inks
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PKD	Public Key Directory
PoP	Proof of Proposal
PWGSC	Public Works and Government Services Canada
RFI	Request for Information
RFID	Radio Frequency Identification

RFP	Request for Proposal
SAC	Supplementary Access Control
SRCL	Security Requirement Checklist

ANNEX 5: SECURITY REQUIREMENT CHECK LIST (SRCL)



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B7021-17-0031 (20170031)
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: Citizenship and Immigration Canada	2. Branch or Directorate / Direction générale ou Direction: CPOC
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: Production of an electonic passport. Various security markings apply.	

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

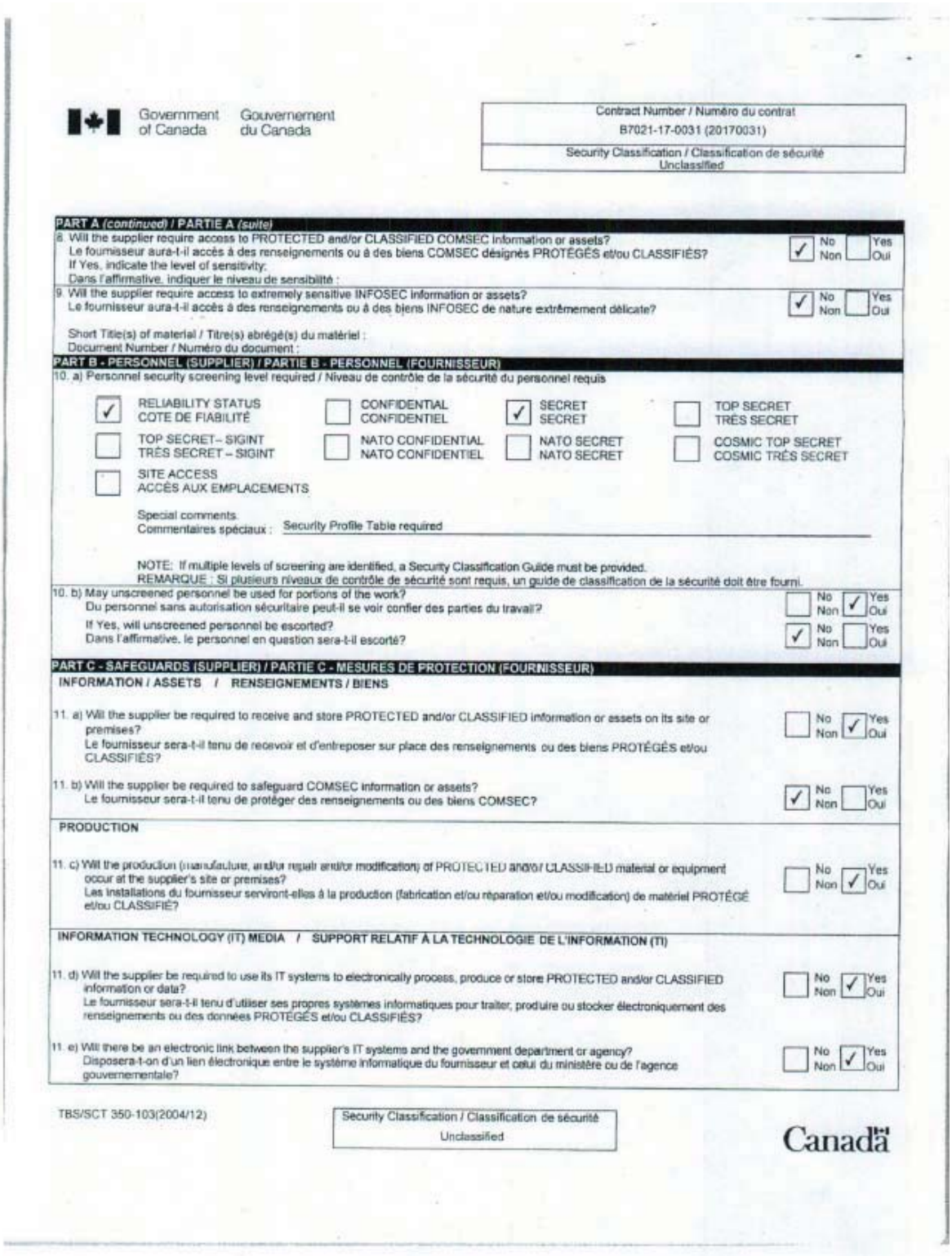
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

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

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité: Unclassified

Canada



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B7021-17-0031 (20170031)

Security Classification / Classification de sécurité
Unclassified

PART A (continued) / PARTIE A (suite)

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

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

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

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

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

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

Special comments / Commentaires spéciaux : Security Profile Table required

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?

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Unclassified

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B7021-17-0031 (20170031)
Security Classification / Classification de sécurité
Unclassified

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

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

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

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

HANDLING INSTRUCTIONS

Transport Standard

TRANSPORT: to physically hand carry protected and classified information from one person/place to another.
Note: The carrier must have the need-to-know.

TYPE OF INFORMATION	RESTRICTED ACCESS AREA	IN CANADA				OUTSIDE CANADA			
		PACKAGING ENCLOSURE				PACKAGING ENCLOSURE			
		None req'd	Single sealed envelope [1, 3]	Double sealed envelope [2, 3]	Single sealed envelope in a secure enclosure (*lockable carrying bag or case*)	None req'd	Single sealed envelope [1, 3]	Double sealed envelope [2,3]	Use an approved dispatch case (*when replacing the outer envelope*)
Protected "A"	Within	X				X			
	Outside		X				X		
Protected "B"	Within	X				X			
	Outside		X				X[7]		
Protected "C"	Within		X				X		
	Outside				X[5,6]			X	X[8]
Confidential	Within	X					X		
	Outside		X				X[7]		
Secret	Within	X					X		
	Outside		X[4]		X[5,6]			X	X[8]
Top Secret	Within		X				X		
	Outside				X[5,6]			X	X[8]

1. When possible, address single and the outer jacket of double sealed envelopes in a non-specific manner (e.g. to departmental mailroom, branch or section), include return address of sender with no security classification of the contents.
2 When double sealed envelopes are used, the outer envelope should be addressed as per note 1. The inner envelope should show the address of the recipient (it may have an attention line with recipient's name), return address of sender and highest security classification of contents.
3 When warranted by the need-to-know, single or inner envelopes should have one of the following restrictive caveats: "TO BE OPENED ONLY BY (position title)"- when only the incumbent of that position is to access the contents, OR "TO BE OPENED ONLY BY (name)"- when only the identified individual is to access the contents (e.g., personal information).
4 It is highly recommended that Secret Information be treated the same as Protected C and Top Secret, due to inadvertent opening while in transit and at security check points.
5 It is highly recommended that this information be placed in a double sealed envelope while in transit and when passing through security check points.
6 When warranted by a TRA that an enhanced security measure (higher assurance of tampering) is required, you may use an approved opaque tamper-indicating security polyethylene envelope with no security markings and placed in a carrying case (carrying bag, backpack, briefcase, etc.)
7 When warranted by a TRA, use a double sealed envelope.
8 You may replace the outer envelope with an approved dispatch case, but it is highly recommended the information be placed in a double sealed envelope.

Transmittal Standard in Canada

TRANSMITTAL: to send protected and classified information from one person/place to another by a third party.

TYPE OF INFORMATION	RESTRICTED ACCESS AREA	PACKAGING ENCLOSURE[1,2]		DELIVERY METHODS	
		Single sealed envelope [3,5]	Double sealed envelope [2,5]	Departmental messenger	Postal or reliable courier service (*when delivery is urgent & essential*)
Protected "A"	Within	X		X	
	Outside	X		X	X
Protected "B"	Within	X		X	
	Outside	X		X	X
Protected "C"	Within	X		X	
	Outside		X	X	X[7]
Confidential	Within	X		X	
	Outside	X		X	X
Secret	Within	X		X	
	Outside	X[6]	X[6]	X	X[7]
Top Secret	Within	X		X	
	Outside		X	X	X[7]

1 You may replace the single or outer sealed envelope with a lockable carrying case (carrying bag, backpack, briefcase, etc.)
2 Note: For bulk shipments, place in a tape-sealed enclosure (envelope, box, etc.) and then place in a locked and/or security-sealed enclosure (crate or transit case). Locks or seals must be applied at the departure point and removed at the reception point by appropriately-screened personnel.
3 When possible, address single and the outer jacket of double sealed envelopes in a non-specific manner (e.g. to departmental mailroom, branch or section), include return address of sender with no security classification of the contents.
4 When double sealed envelopes are used, the outer envelope should be addressed as per note 1. The inner envelope should show the address of the recipient (it may have an attention line with recipient's name), return address of sender and highest security classification of contents.
5 When warranted by the need-to-know, single or inner envelopes should have one of the following restrictive caveats: "TO BE OPENED ONLY BY (position title)"- when only the incumbent of that position is to access the contents, OR"TO BE OPENED ONLY BY (name)"- when only the identified individual is to access the contents (e.g., personal information).
6 It is highly recommended that Secret information be transmitted in a double sealed envelope.
7 If departmental messenger service is not available and delivery is urgent, essential and approved by the DSO on a case-by-case basis, use these services, with the option of a signature upon delivery (this method greatly increases the risk of compromise).

Transmittal Standard outside Canada

TRANSMITTAL: to send protected and classified information from one person/place to another by a third party. Note: The bearer does not have the need-to-know. Outside Canada means to, from or within GoC facilities (i.e. embassies, missions or deployments, GoC buildings, consulates etc.) in foreign countries.

TYPE OF INFORMATION	RESTRICTED ACCESS AREA	PACKAGING ENCLOSURE[1,2]		DELIVERY METHODS[6]		
		Single sealed envelope [3,8]	Double sealed envelope [4,5]	Departmental messenger	DFAIT Diplomatic Mail Service	Postal or reliable courier service (*when delivery is urgent & essential*)
Protected "A"	Within	X		X		
	Outside	X		X	X	X[11]
Protected "B"	Within	X		X		
	Outside	X		X	X	X[11]
Protected "C"	Within	X	X[7]	X		
	Outside		X[9]	X[10]	X	
Confidential	Within	X		X		
	Outside	X[8]		X[10]	X	X[12]
Secret	Within	X	X[7]	X		
	Outside		X[9]	X[10]	X	
Top Secret	Within	X	X[7]	X		
	Outside		X[9]	X[10]	X	

1 You may replace the single or outer sealed envelope with an approved dispatch case listed in the RCMP Security Equipment Guide (SEG).
2 Note: For bulk shipments, place in a tape-sealed enclosure (envelope, box, etc.) and then place in a locked and/or security sealed enclosure (crate or transit case). Locks or seals must be applied at the departure point and removed at the reception point by appropriately-screened personnel.
3 When possible, address single and the outer jacket of double sealed envelopes in a non-specific manner (e.g. to departmental mailroom, branch or section), include return address of sender with no security classification of the contents.
4 When double sealed envelopes are used, the outer envelope should be addressed as per note 1.The inner envelope should show the address of the recipient (it may have an attention line with recipient's name), return address of sender and highest security classification of contents.
5 When warranted by the need-to-know, single or inner envelopes should have one of the following restrictive caveats:"TO BE OPENED ONLY BY (position title)"- when only the incumbent of that position is to access the contents, OR "TO BE OPENED ONLY BY (name)"- when only the identified individual is to access the contents (e.g., personal information).
6 When protected and classified information is transmitted to, from or within foreign countries and particularly in non NATO countries, the use of DFAIT Diplomatic Mail Services is very strongly recommended.
7 It is highly recommended that this information be placed in a double sealed envelope in case of advertent opening.
8 Use a double sealed envelope when transmitting by DFAIT Diplomatic Mail Services.
9 Place a Transmittal Note and Receipt form in the inner envelope and seal with approved security tape specified in the RCMP Security Equipment Guide (SEG).
10 Transmit only by appropriately-screened services and when delivery is urgent, essential and approved by the DSO.
11 If DFAIT Diplomatic Mail Services and departmental messenger service is not available and as approved by the DSO on a case-by-case basis, use these services, with the option of a signature upon delivery (this method greatly increases the risk of compromise).
12 This method only applies to the USA and the UK.

Protected Information

(Information sensitive to personal or commercial interest.)

	INFORMATION RELEASED COULD CAUSE	EXAMPLES OF PROTECTED INFORMATION	ELECTRONIC TRANSFERS (e.g., E-mail, FTP)	STORAGE	LAPTOP	COMMUNICATION ACROSS CANADA AND TO THE MISSIONS	DISPOSAL
A	• Minor injury • Embarrassment for an individual, a company or the Government of Canada	Personal • Date of birth** • Home address** and telephone number** • Salary** • SIN** • Fingerprint** • Photo** Organization • Contract number** • Standing offers	• May be emailed between government departments and agencies without any additional safeguards.	• CIC Network drives (personal and shared drive) • Appropriately labelled media***	Save on: • Hard drive (C:\) or other appropriately labelled media***	• Use a regular telephone and a regular fax	• Overwrite/ format media ***
B	• Medium to serious injury • Detriment, harm • Financial loss or gain for an individual, a company or the Government of Canada	Personal • Performance evaluation • Medical/ Psychiatric information • Contractual information • Financial information • Harassment investigation Organization • Trade secrets of a third party • Contractual information • Competitive position of a third party • Most CIC client files	• May be transmitted within CIC across Canada. • Outside CIC, must use approved Government of Canada encryption software. Missions: • Consult the security officer	• CIC Network drives (personal and shared drive) • Appropriately labelled media*** • Store all media*** in a secure cabinet • Data on removeable and portable media must be encrypted with Government of Canada approved encryption tools.	Save on: • Hard drive (C:\) with approved Government of Canada encryption software. • Copy must also exist on CIC corporate network. • Consult the IT Security Unit	• Use a regular telephone and a secure fax approved by the Government of Canada (*) • Use discretion on cellular telephone Missions: • Use a secure telephone and secure fax	• Send media*** to the IT Security Unit for disposal or demagnetizing (degauss) Missions: • Give to the security officer for disposal
C	• Extremely serious injury • Loss of life • Significant financial loss or gain for an individual, a company or the Government of Canada	• Witness Protection Program • Security plans for protecting very valuable assets	• Transmission must be on a secure network, not on the CIC protected B network • Use a dedicated printer Missions: • Consult the security officer	• Store only on a secure network or on a standalone PC with a removable hard drive that has been encrypted with Government of Canada approved encryption tools. • Store data on media***, with the appropriately label, in an approved secure cabinet (safe) • Use a dedicated printer	• Consult the IT Security Unit	• Use a secure telephone and secure fax approved by the Government of Canada (*) • For the use of a secure cellular telephone, consult with the COMSEC custodian Missions: • Use a secure telephone and secure fax	• Send media*** to the IT Security Unit for disposal Missions: • Give to the security officer for disposal

*** Secure Telephone Units and secure fax approved by the Government of Canada - conversations and fax transmissions are encrypted when using these equipment. Contact your COMSEC Custodian.**
****Data elements may be individually classified as Protected A. Combining these elements, that uniquely identifies an individual(s), may raise the classification above Protected B.**
***** Floppy, CD, Hard Disk, Memory stick, etc.**

Classified Information

(Information sensitive to national security or of national interest.)

	INFORMATION RELEASED COULD CAUSE	EXAMPLES OF PROTECTED INFORMATION	ELECTRONIC TRANSFERS (e.g., E-mail, FTP)	STORAGE	LAPTOP	COMMUNICATION ACROSS CANADA AND TO THE MISSIONS	DISPOSAL
CONFIDENTIAL	• Minor injury • Classified information that merits this level is limited	• Information related to negotiations with provincial governments	• Transmission must be on a secure network, not on the CIC protected B network • Use a dedicated printer	• Store only on a secure network or on a standalone PC with a removable hard drive • Store data on media***, with the appropriate label, in an approved secure cabinet • Use a dedicated printer Missions: • Consult the security officer	• Consult the IT Security Unit	• Use a secure telephone and secure fax (*) approved by the Government of Canada with a Confidential key • For the use of a secure cellular telephone, consult with the COMSEC custodian	• Send media*** to the IT Security Unit for disposal Missions: • Give to the security officer for disposal
SECRET	• Serious injury • Most classified information falls in this category	• Information exchange and negotiations with foreign governments • Advice and recommendations to the Minister • Cabinet Documents • Financial Documents • Case files with national security implications	• Transmission must be on a secure network, not on the CIC protected B network • Use a dedicated printer Missions: • Consult the security officer (C5)	• Store only on a secure network or on a standalone PC with a removable hard drive • Store data on media***, with the appropriate label, in an approved secure cabinet (safe) • Use a dedicated printer Missions: • Consult the security officer	• Consult the IT Security Unit	• Use a secure telephone and secure fax (*) approved by the Government of Canada with a Secret key • For the use of a secure cellular telephone, consult with the COMSEC custodian	• Send media*** to the IT Security Unit for disposal Missions: • Give to the security officer for disposal
TOP SECRET	• Exceptionally serious injury • Information that merits this level is very limited	• International treaties and agreements • Law enforcement and immigration intelligence • Operational plans or political negotiations • Scientific and technical data connected to the defence of the nation or allied nations	• Transmission must be on a secure network, not on the CIC protected B network • Use a dedicated printer	• Store only on a secure network or on a standalone PC with a removable hard drive • Store data on media***, with the appropriate label, in an approved secure cabinet (safe) • Use a dedicated printer Missions: • Consult the security officer	• Consult the IT Security Unit	• Use a secure telephone and secure fax (*) approved by the Government of Canada with a Top Secret key • For the use of a secure cellular telephone, consult with the COMSEC custodian	• Send media*** to the IT Security Unit for disposal Missions: • Give to the security officer for disposal

*** Secure Telephone Units and secure fax approved by the Government of Canada - conversations and fax transmissions are encrypted when using these equipment. Contact your COMSEC Custodian.**
**** For delivery outside Canada, consult the IT Security Unit.**
***** Floppy, CD, Hard Disk, Memory stick, etc.**

ATTACHMENT 1 TO PART 5: MANDATORY EVALUATION CRITERIA

Suppliers must meet all of the mandatory requirements in this attachment. In accordance with Part 5 - Evaluation Procedures and Basis of Qualification of the ITQ, Canada may contact the client contact for the referenced project(s) to validate Supplier's responses.

1.1 Substantiation of Technical Compliance – Mandatory Evaluation Criteria

1.1.1 Suppliers must respond to the corresponding mandatory requirements by providing a description explaining, demonstrating, substantiating and justifying their Qualifications. Suppliers are requested to utilize the unique number and associated title of each mandatory requirement in their responses. Suppliers are requested to indicate where their mandatory requirement is met by entering the location (e.g. volume/binder number, page number, etc.) in the "Cross Reference to Response" column. Supplier's responses to the mandatory requirements will be evaluated as either "Met" or "Not Met". A "Not Met" will result in the response being deemed non-responsive.

1.1.2 Suppliers are requested to submit "**Form 2 – Project Reference Check Form**", for each project claimed in response to corresponding mandatory requirement(s).

1.1.3 Suppliers should only provide the required reference project(s) as indicated in each mandatory requirement. If more than the required number of reference project(s) is provided, the Suppliers will be required to clarify which reference project(s) apply to corresponding mandatory requirement(s).

1.1.4 Please refer to "**Annex 3 – Glossary of Terms**" to assist with responding to the mandatory requirements.

Req #	Mandatory Requirement	Cross Reference to Response
M1	The Supplier must be the manufacturer of the Blank Travel Documents as required by Canada. Suppliers must demonstrate compliance with this requirement by: (a) Providing a description of the corporate structure of the Supplier that clearly identifies the role of the Supplier as the manufacturer of the Blank ePassport Books. In the case of a joint venture, identifying the organization which will have the primary responsibility for the manufacturing of the Blank ePassport books under any Contract resulting from this procurement process; and (b) Identifying and defining the relationship between the Supplier, the Core Team, and the providers of products or services required by the Supplier to meet the requirements of Canada as expressed in this ITQ.	

M2	The Supplier must have the capability to design, develop, manufacture and assemble the ICAO compliant Canadian ePassport and other electronic and non-electronic Travel Documents. Suppliers must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have designed, developed and manufactured ICAO compliant ePassports; and (b) Providing a sample of that product. Where the Reference Project provided to demonstrate compliance with criterion M2 is that of a member of the Supplier's Core Team, in addition to the requirements above, the Supplier must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M3	The Supplier must have the capability to design, develop and implement an ICAO compliant Canadian ePassport Personalization System. Suppliers must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have designed, developed and implemented an ICAO compliant ePassport Personalization System. Where the Reference Project provided to demonstrate compliance with criterion M3 is that of a member of the Supplier's Core Team, in addition to the requirement above, the Supplier must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M4	The Supplier must have experience in the implementation of an ICAO compliant ePassport PKI Solution. Suppliers must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have implemented an ICAO compliant PKI Solution. Where the Reference Project provided to demonstrate compliance with criterion M4 is that of a member of the Supplier's Core Team, in addition to the requirement above, the Supplier must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M5	The Supplier must have an existing facility or must be in the process of obtaining a facility within Canada to manufacture the ICAO compliant Canadian ePassport and other electronic and non-electronic Travel Documents as of the closing date of the ITQ. Suppliers must demonstrate compliance with this requirement by providing for each facility proposed in the design, manufacture and storage of the Canadian Travel Documents covered under this ITQ either: (a) A copy of a valid Facility Security Clearance certificate at the level of SECRET issued by the Canadian Industrial Security Directorate (CISD) of the Department of Public Works and Government Services Canada (PWGSC); or, (b) A copy of the completed submission documents to obtain Facility Security Clearance certificates at the level of SECRET issued by the Canadian and International Industrial Security Directorate (CISD) of the Department of Public Works and Government Services Canada (PWGSC) accompanied by an attestation from the Supplier confirming that the documents were submitted to CISD before the closing date of the ITQ. Canada will contact CISD to confirm the submission documents have been received by CISD prior to the ITQ closing date. Should there be no record of the documentation being received by CISD prior to the ITQ closing date, the Supplier will be deemed as not having demonstrated compliance with this criteria.	
M6	The Supplier must be located in Canada or in a country which has a bilateral industrial security agreement with Canada. Currently, Canada's Industrial Security Program has international bilateral industrial security instruments with the countries listed on the following PWGSC Web site: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html (a) Suppliers must demonstrate compliance with this requirement by providing proof that the Supplier's head office is located in a country with which Canada's Industrial Security Program has a bilateral industrial security agreement.	
M7	Canada will have two (2) central print centers with high-volume printers and several regional print sites with low-volume printers (See Annex 1). The Supplier must be able to furnish the personalization equipment for a decentralised printing model with high-volume and low-volume solutions. Suppliers must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have furnished the personalization equipment for an issuing state that operates a hybrid issuance model with a minimum of one (1) centralized personalization site with a high-volume printer and a minimum of three (3) regional personalization sites with a Low-Volume Printer.	

	Where the Reference Project provided to demonstrate compliance with criterion M7 is that of a member of the Supplier's Core Team, in addition to the requirement above, the Supplier must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M8	The Supplier must have the capacity to manufacture a high-volume of ePassport books containing laser engraveable polycarbonate data pages. Suppliers must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have manufactured, within a 12 month period, at least a total of 2 million travel documents in a booklet format that were required by the issuing state to be compliant with ICAO Document 9303 standards for electronic machine readable travel documents; and (b) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have manufactured, within a 12 month period, at least a total of 4 million travel documents in a booklet format that were required by the issuing state to be compliant with ICAO Document 9303 standards for machine readable travel documents (regardless of whether they were electronic or not); and (c) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team have manufactured travel documents in a booklet format containing a laser engraveable polycarbonate data page that were required by the issuing state to be compliant with ICAO Document 9303 standards for electronic machine readable travel documents. This requirement explicitly excludes TD-2 and TD-1 (or ID-1) format documents as well as visas, none of which will be accepted as proof of experience. Where the Reference Project provided to demonstrate compliance with criterion M8 is that of a member of the Supplier's Core Team, in addition to the requirement above, the Supplier must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

FORM 1: ITQ SUBMISSION FORM

#	Response
	Supplier's full legal name
(a)	
	Supplier's Procurement Business Number
(b)	
	Authorized Representative of Supplier for evaluation purposes (e.g. clarifications)
(c)	Name:
	Title:
	Address:
	Telephone #:
	Email:
	If submitting a response to the ITQ as a joint venture, the Supplier must provide the joint venture member's full legal name and address [*Supplier to add more rows if more than two (2) joint venture members*]
(d)	Joint venture member full legal name:
	Joint venture member address:
(e)	Joint venture member full legal name:
	Joint venture member address:
	Canada's Official Language in which the Supplier will communicate with Canada during the ITQ process – indicate either English or French
(f)	☐ **English** ☐ **French**
	Core Team Members
Core Team Member 2 full legal name:	
Address:	
Core Team Member 3 full legal name:	
Address:	

Core Team Member 4 full legal name:	
Address:	
ITQ Submission Requirements **It is the Suppliers sole responsibility to ensure their response addresses all requirements outlined in the ITQ.**	
Supplier Authorization	
(h)	Name:
	Address:
	Email:
	Signature of authorized representative of Supplier
	Telephone #:
	Date:
If submitting a response to the ITQ as a joint venture, the Supplier must complete section (h) below. **[*Supplier to add more rows if more than two (2) joint venture members*]**	
(h)	Name:
	Address:
	Email:
	Signature of authorized representative of Supplier
	Telephone #:
	Date:

FORM 2: PROJECT REFERENCE CHECK FORM

Instructions to Suppliers:

(a) Suppliers are requested to submit a Project Reference Check Form for each project referenced in response to each mandatory requirement in Attachment 1 to Part 5 of the ITQ.

(b) If the information requested in this form is not provided with the Suppliers' ITQ response it must be provided upon request by the Contracting Authority within the timeframe identified in the request.

(c) Canada may contact the client contact, provided for the referenced project, to validate the information provided.

#	Response		
(a)	Mandatory Requirement Number (from Attachment 1 to Part 5)		
(b)	Supplier Full Legal Name (if the Supplier is a joint venture, the full legal name of the joint venture member for the referenced project)		
(c)	Description of the referenced project		
(d)	Name of client organization for the referenced project		
(e)	Name of client contact for the referenced project		
(f)	Client organization and client contact affiliation with the Supplier (or joint venture member)		
	Please indicate accordingly	Are Not Affiliated	Are Affiliated
(g)	Name of organization the client contact is currently working for (if the client contact is no longer working for the client organization identified for the referenced project)		
(h)	Title of client contact (while working on the referenced project)		
(i)	Current telephone number of client contact		
(j)	Current e-mail address of the client contact		
(k)	Role of the client contact in the referenced project		