RETURN BIDS TO:

IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca

Attn: Jodie Thomas

FOR ELECTRONIC BIDS:
The electronic mailbox is equipped to send an automatic reply to all messages received. If you do not receive an automatic response, please contact the Contracting Authority to ensure your bid was received. Please note that it is the bidder's sole responsibility to ensure that all bids submitted are received in their entirety by Citizenship and Immigration Canada by the closing date and time indicated in this RFP.

IMPORTANT NOTICE TO SUPPLIERS
The Government Electronic Tendering Service on canadabuys.canada.ca/en/tender-opportunities will be the sole authoritative source for Government of Canada tenders that are subject to trade agreements or subject to departmental policies that require public advertising of tenders.

REQUEST FOR PROPOSAL
Proposal To: Citizenship and Immigration Canada
We hereby offer to sell to His Majesty the King in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out thereof.

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT

Instructions : See Herein
Instructions: Voir aux présentes
Issuing Office – Bureau de distribution
Citizenship and Immigration Canada
Procurement and Contracting Services
70 Crémazie
Gatineau, Québec K1A 1L1

Title – Sujet Cloud based Enterprise Learning Management System (LMS) for department wide use at Immigration, Refugees and Citizenship Canada	
Solicitation No. – N° de l'invitation **CIC-152202 - B**	**Date** **October 20 2022**
Solicitation Closes – L'invitation prend fin at – à *2:00* **PM** **on – November 15 2022**	**Time Zone** **Fuseau horaire** **EST**
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Inquiries to: - Adresser toutes questions à : **IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca**	
Telephone No. – N° de téléphone : **343-554-7603**	
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction :** See Herein	
Delivery required - Livraison exigée ***See Herein***	
Vendor/firm Name and address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Facsimile No. – N° de télécopieur** **Telephone No. – N° de téléphone**	
Name and title of person authorized to sign on behalf of Vendor/firm **Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur** _____ **(type or print)/ (taper ou écrire en caractères d'imprimerie)** _____ _____ **Signature** **Date**	

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

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

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

1.2 Summary

1.2.1 This bid solicitation is being issued to fulfill the requirement of Citizenship and Immigration Canada, hereinafter known as Immigration, Refugees and Citizenship Canada (IRCC) to acquire a web-based Software as a Services model Learning Management System (LMS) that can be configured to meet specific IRCC requirements and allows for the management, delivery, tracking, reporting and evaluation of all training and learning content.

The end state will be a cloud-based, browser accessed technology-enabled system, available to up to 15,000 departmental employees. This system will allow employees to consume learning content while maintaining and tracking their progress. The cloud-based application/system must provide a streamlined and enhanced end-to-end learning experience and allow effective, complete, and overall control of learning content management, robust analytics, administration, and communication with learners, learning providers, and decision makers. For the purposes of this solicitation, Bidders must meet the security requirements identified under *Tier 1 – Security Requirements for SaaS.*

1.2.2 Single Contract

Canada is seeking to establish a contract for a Learning Management System (LMS) for which a portion of the work will be on an “as and when requested” basis, as defined in Appendix D, Statement of Work, for six (6) years including all options.

1.2.3 Security Requirements

There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, Part 7 - Resulting Contract Clauses, Appendices F and G. For more information on personnel and organization security screening or security clauses, bidders should refer to the Contracting Security Program of Public Works and Government Services Canada Security requirements for contracting with the Government of Canada.

1.2.4 Trade Agreements

The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), the Canadian Free Trade Agreement (CFTA), the Canada-Columbia Free Trade Agreement (CColFTA), the Canada-Chile Free Trade Agreement (CCFTA), The Canada-Peru Free Trade Agreement (CPFTA), the Canada-Panama Free Trade Agreement (CPanFTA), and the Canada-Honduras Free Trade Agreement (CHFTA).

1.2.5 Task Authorizations

This bid solicitation is to establish a contract with task authorizations for the delivery of the requirement detailed in the bid solicitation to the Identified Users across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside the resulting contract.

1.2.6 Federal Contractors Program (FCP)

The Federal Contractors Program (FCP) for employment equity applies to this procurement; see Part 5 Certifications and Additional Information, Part 7 - Resulting Contract Clauses.

1.2.7 Accessibility

Considering accessibility criteria and features is obligatory with this requirement. For additional information consult the *Treasury Board Contracting Policy*.

1.2.8 Diversity

IRCC is committed to achieving a procurement process that reflects the diversity of Canada. We are dedicated to identifying and reducing barriers in our procurement processes. We continue to work on improving practices that will help ensure that equity group members are well-represented. To this end, minority-owned businesses are encouraged to apply to our processes.

1.3 Debriefings

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

If you have any concerns relating to the procurement process, please refer to the Bid Challenge and Recourse Mechanisms page on the CanadaBuys.canada.ca website. Please note that there are strict deadlines for filing complaints with the Canadian International Trade Tribunal (CITT) or the Office of the Procurement Ombudsman (OPO).

1.4 Mandatory Requirements

Where the words “must”, “shall” or “will” appear in this RFP, the clause is to be considered as a mandatory requirement.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All Immigration, Refugees and Citizenship Canada (IRCC) instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out on the IRCC Website.

All SACC manual clauses for specific instructions not covered by the standard instructions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual issued by Public Works and Government Services Canada.

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

The CIC-SI-001 (2016-05-26) Standard Instructions – Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of CIC-SI-001 (2016-05-26) Standard Instructions – Goods or Services – Competitive Requirements, is amended as follows:

Delete: 90 days
Insert: 250 days

2.2 Submission of Bids

Bids must be submitted only to Immigration, Refugees and Citizenship Canada by the date, time and place indicated on page 1 of the bid solicitation.

Due to the nature of the bid solicitation, bids transmitted by epost Connect service and by facsimile will not be accepted.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the bid closing date. Enquiries received after that time may not be answered.

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

2.4 Applicable Laws

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

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

2.5 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion.

Suggestions that do not restrict the level of competition nor favor a particular bidder will be given consideration provided they are submitted to the Contracting Authority **at least five (5) days** before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.6 Former Public Servant

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, bidders 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 bids is completed, Canada will inform the Bidder 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 Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

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

Work Force Adjustment Directive

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

If so, the Bidder must provide the following information:

a. name of former public servant;
b. conditions of the lump sum payment incentive;
c. date of termination of employment;
d. amount of lump sum payment;
e. rate of pay on which lump sum payment is based;
f. period of lump sum payment including start date, end date and number of weeks;
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.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

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

Section I: Technical Bid (one (1) electronic copy via email)
Section II: Financial Bid (one (1) electronic copy via email)
Section III: Certifications and Additional Information (one (1) electronic copy via email)
Section IV: Supply Chain Integrity Information (one (1) electronic copy via email)

Due to the nature of the bid solicitation, bids transmitted by epost Connect services and by facsimile will not be accepted. In accordance with section 2.2, bids shall be transmitted by electronic mail.

Canada requests that respondents submit their response in unprotected (i.e. no password) PDF format by email. Complete size of emails containing a response must not exceed 10MB. Emails exceeding 10MB will not be received. Should the size of email(s) exceed 10MB, respondents must contact the Contracting Authority at least 48 hours prior to the closing date to discuss alternatives.

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

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

(a) use a numbering system that corresponds to the bid solicitation; and
(b) page numbering must be used on the bottom right of each page of the proposal

3.2 Section I: Technical Bid

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

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

c) The technical bid consists of the following:

i **Substantiation of Technical Compliance:** The Technical Bid must substantiate the compliance of the Bidder's LMS Service with *Annex A to Appendix D - Statement of Requirements.*

ii **SaaS Publisher Certification Form (Form 1) -** If the SaaS Publisher (defined as the entity or person who is the owner of the copyright in any SaaS Solution included in the Submission and who has the right to the license and to authorize others to use its SaaS Solution and any underlying components) intends to submit a Submission and qualify itself as a Supplier, such SaaS Publishers must submit the certification Form 1.

iii **SaaS Publisher Authorization Form (Form 2)** – If an entity other than the SaaS Publisher who is authorized to distribute and re-sell the SaaS Solutions(s) intends to submit a Submission and qualify itself as a Supplier, such entity must submit certification from the SaaS Publisher, in accordance with Form 2, to certify that such entity has been authorized to supply the SaaS Solution Publisher's SaaS Solution(s).

iv **Substantiation of Compliance with Tier 1 Security Requirements:** Bidders must substantiate compliance with the Tier 1 security requirements contained in *Appendix L – Tier 1 Security*

Requirements. The substantiation must not simply be a repetition of the requirements, but must explain and demonstrate how the Supplier meets the requirements. Simply stating that the Supplier or its proposed SaaS Solutions comply is not sufficient. Where Canada determines that the substantiation is not complete, Canada will provide the Supplier with an opportunity to submit the required substantiation.

v **Technical Documentation:** The Bidder must provide technical documentation such as user manuals, screenshots, design or system management documents (or other information sources) to support the Bidder's response to each requirement identified in *Annex A to Appendix D - Statement of Requirements* (an electronic copy of the technical documentation to support the technical bid is acceptable). The Technical Documentation must demonstrate how the Bidders proposed solution meets the mandatory criteria. Links to websites are not acceptable and if provided to validate a mandatory requirement, it will render the bid response non-responsive. The Bidder must include the precise location of the reference material including the title of the document, the page and the paragraph numbers when addressing each criterion. Any reference material listed by the Bidder to demonstrate the compliance must be part of the bid. If it is not included in the bid, it will not be taken into consideration by Canada. Where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the bid documentation.

vi **Service Level Agreements:** Bidders must submit their published Service Level Agreements (SLAs), to be included in Appendix J – SaaS Solution Level Agreements (SLAs).

The service level commitments (detailed in the published SLAs) must provide commercial clients support which includes, at the minimum, any published and commercially available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the SaaS Solution.

The following are examples of terms that may be addressed in the Bidder's SLA:

A. Period during which the Bidder will support the Client;
B. Contact and procedure information for accessing support;
C. Procedures for resolution of problems;
D. Response times;
E. Procedures on how and when all telephone or email communications will be responded to;
F. Website support availability to Clients (e.g. 24 hours a day, 365 days a year, and 99.9% of the time); and,
G. Maintenance entitlements (e.g. patches, updates, major/minor releases, etc.)

By presenting a Submission, the Bidder acknowledges and agrees that any terms contained in Appendix J - SaaS Solution Service Level Agreements that purport to interpret the Contract, are the same or similar subject matter, or are related to the terms contained in the Resulting Contract Clauses, are deemed stricken and are of no force or effect

vii **Compliance with Appendix G – Security & Privacy Obligations:** Bidders must comply with security and privacy obligations contained in Appendix G – Security & Privacy Obligations. Bidders must demonstrate that they meet the security and privacy obligations detailed under Appendix G by responding to the mandatory requirements detailed in Appendix L – Tier 1 Security Requirements for SaaS. Suppliers may be requested to demonstrate their ongoing compliance with Annex B – Security & Privacy Obligations upon request throughout the period of the Contract.

By presenting a bid, the bidder acknowledges and agrees that all other terms submitted as part of the Technical Submission are deemed stricken and form no part of the contract.

3.3 Section II: Financial Bid

a) In the Financial bid, Bidders must submit the proposed SaaS Solution with their commercial pricing and any prices or rates applicable for professional services to be provided by the Bidder. It is required that the SaaS Solutions and Commercial Prices section of the Submission be presented as per the Pricing Schedule provided in **Appendix E, Basis of Payment**. The Financial Submission should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Submission will be evaluated.

b) The following must be addressed in **Appendix E, Basis of Payment:**

i. **SaaS Publisher's Part No.:** Bidders should provide the part number that the SaaS Publisher uses to identify the SaaS Solution commercially;

ii. **SaaS Solution's Name:** Bidders must provide the commercial name that the SaaS Publisher uses to identify the SaaS Solution commercially.

iii. **SaaS Publisher's Name:** Bidders must provide the name of the SaaS Publisher that owns the Intellectual Property rights to the SaaS Solution;

iv. **Cloud Service Provider (CSP)'s name:** Bidders must identify the existing Cloud Service Provider (CSP) that hosts the proposed SaaS Solution.

v. **Prices:** Bidders must submit prices for the SaaS Solution and any applicable professional services proposed in Appendix E, Basis of Payment.The prices must be:

A. the Bidder's commercial pricing
B. in Canadian dollars; and,
C. exclusive of Goods and Services Tax or Harmonized Sales tax.

vi. **Unit of Measure:** Bidders must enter the unit of measure for their SaaS Solution Price (such as "per user", "per entity", etc.) under which the SaaS Solutions will be provided to Canada;

vii. **Language(s) available:** Bidders must indicate the language(s) under which the SaaS Solution is available, designated as "EN" for English, "FR" for French, or "EN, FR" for both;

Bidders must submit their financial bid in accordance with Appendix E, Basis of Payment. The total amount of applicable taxes must be shown separately, if applicable.

Bidders should include the following information in their financial bid by completing Appendix N, Vendor Information and Authorization and include it with their bid:

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

Financial proposals must clearly identify the personnel proposed and the associated category for evaluation purposes only. Proposed per diem rates or firm prices must be in Canadian dollars.

The Bidder's rates in response to this RFP and resulting contract(s) must include all overhead, general & administrative costs and profit. Included are the following costs that may be incurred in providing the required services: computer hardware and software, word processing, preparation of reports, photocopying, courier services, facsimile services, telephone services, local travel expenses, and administration related to non-local travel expenses. Local as used here is defined as where the Work is to be performed in Canada as may be specified in the RFP and the resulting Contract(s).

Bidders must provide in their financial bid a price breakdown as detailed in Appendix E, Basis of Payment.

CHANGES MADE TO APPENDIX E, BASIS OF PAYMENT WILL RENDER THE BID NON-COMPLIANT.

SACC Manual Clauses

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

The requirement does not provide for exchange rate fluctuation protection. Any request for exchange rate fluctuation protection will not be considered and will render the bid non-responsive.

3.5 Section III: Certifications and Additional Information

Bidders must submit the required certifications and additional information required under Part 5.

3.6 Section IV: Supply Chain Integrity (SCI) Requirements

a) Bidders must submit specific information regarding each component of their proposed solution's Supply chain ("Supply Chain Security Information" or "SCSI") as defined in section 1.1 of Appendix H, Supply Chain Integrity Process.

b) Bidders must submit Supply Chain Security Information (SCSI) detailed in **Form 3 – SCSI Vendor Submission form**, and must keep current, or update any SCSI as required by the Supply Chain Security Authority. The Supply Chain Security Information will be used by Canada to assess whether, in its opinion" a Bidder's proposed supply chain creates the possibility that the Bidder's proposed SaaS Solution could compromise or be used to compromise the security integrity of Canada's requirement, firmware, software, systems or information in accordance with the Supply Chain Integrity Process as described in section **Appendix H Supply Chain Integrity Process.**

c) By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Bidder agrees to the terms of the non-disclosure agreement contained in **Annex K Non-Disclosure Agreement related to the Supply Chain Integrity.**

d) Bidders must submit **Form 4 - Cloud SaaS Technical SCI Assessment controls Supplier Questionnaire** and must provide authenticated and certified information for the Cyber Security control and assessment to ascertain coherence to Supply Chain Integrity. Bidders must substantiate compliance to each claim with a certified certificate.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

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

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

(c) **Requests for Clarifications:** If Canada seeks clarification or verification from a Bidder about its Submission, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet any deadline will render the Submission non-responsive, on "hold", or will create delay in processing contract award.

(d) Right of Canada:

a. In the event of a sole compliant bid, Canada reserves the right to reject any SaaS Solution proposed by a Bidder and enter into negotiation related to any prices under Appendix E, Basis of Payment;
b. In the event of a sole compliant bid, Canada reserves the right to reject or negotiate any of the terms and conditions proposed by a Bidder and submitted under Appendix J, Service Level Agreement (SLA). No contract will be awarded unless and until Canada has approved all such terms and conditions

4.2 Technical Evaluation

4.2.1 Mandatory Technical Criteria

The bid **must** meet the mandatory technical criteria specified in Annex A to Appendix D *Statement of Requirements - Bidder Response TABLE A - Mandatory Requirements*. The Bidder must submit the necessary documentation to support compliance with this requirement.

Mandatory requirements are evaluated on a simple pass or fail basis. Failure by a Bidder to meet any one of the mandatory requirements will render the Bidder's proposal **non-responsive and will not be given further consideration.** The treatment of mandatory requirements in any procurement process is absolute. Each mandatory technical criterion should be addressed separately.

The mandatory technical requirements are as follows:

i Technical Documentation as per Article 3.2 (c) (v);
ii Substantiation of compliance with Annex A to Appendix D Statement of Requirements – Bidder Response Table A – Mandatory requirements;
iii Substantiation of compliance with Tier 1 Security Requirements as per Article 3.2(c)(iv);
iv Service Level Agreement as per Article 3.2 (c) (vi); and
v Certifications as per Part 5;

4.2.2 Point Rated Technical Criteria

Each Technical Bid that meets all the Mandatory Requirements specified above will be evaluated and scored in accordance with the point-rated evaluation criteria table specified in Annex A to Appendix D *Statement of Requirements - Bidder Response TABLE B - Rated Requirements.* Each point rated technical criterion should be addressed separately.

4.3 Financial Evaluation

Only the proposals that are technically responsive will be considered for financial evaluation.

The price of the bid will be evaluated in Canadian dollars, applicable taxes are excluded.

For the purposes of bid evaluation, Appendix E - Basis of Payment will be used. The Bidder must provide all-inclusive firm unit prices for the Cloud and associated professional services being proposed in accordance with the bid solicitation, for the initial contract period and option periods.

The volumetric data included in the pricing schedule detailed in Appendix E, Basis of Payment is provided for bid evaluated price determination purposes only. They are not to be considered as a contract guarantee.

The "TOTAL EVALUATED PRICE" in Annex E, Basis of Payment, excluding taxes, will be used to determine the financial evaluation score.

The "TOTAL EVALUATED PRICE" in Appendix "E", Basis of Payment will be calculated by adding the initial contract period total (Tables 1 and 2) and the Option Period totals (Tables 3 and 4). The sum of the four tables will be used to determine the financial evaluation.

Table 5, Optional Additional Users Access will not be included in the financial evaluation, however, should any items be exercised during the initial period or option years, the pricing must not exceed an increase of 3% per year.

4.3.1 Formulas in Pricing Schedule

If the Pricing Schedule provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a bidder.

4.3.2 Substantiation of Professional Services Rates

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates for professional services bids, Canada may, but will have no obligation to, require price support for any rates proposed (either for all or for specific resource categories). Examples of price support that Canada would consider satisfactory include:

a) documentation (such as billing records) that shows that the Bidder has recently provided and invoiced another customer (with whom the Bidder deals at arm's length) for services similar to the services that would be provided by the relevant resource category, where those services were provided for at least one month and the fees charged are equal to or less than the rate offered to Canada (to protect the privacy of the customer, the Bidder may black out the customer's name and personal information on the invoice submitted to Canada);
b) a signed contract between the Bidder and an individual qualified (based on the qualifications described in this bid solicitation) to provide services under the relevant resource category, where the amount payable under that contract by the Bidder to the resource is equal to or less than the rate bid for that resource category;
c) a signed contract with a subcontractor who will perform the work under any resulting contract, which provides that the required services will be provided at a rate that is equal to or less than the rate bid for the relevant resource category (and where the resource meets all the qualifications described in this bid solicitation); or
d) details regarding the salary paid to and benefits provided to the individuals employed by the Bidder qualified (based on the qualifications described in this bid solicitation) to provide services under the relevant resource category where the amount of compensation, when converted to a per diem or hourly rate (as applicable), is equal to or less than the rate bid for that resource category.

Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (either the information described in the examples above, or other information that demonstrates that it will be able to recover its own costs based on the rates it has proposed) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid, while, at a minimum, recovering its own costs. Where Canada determines that the information provided by the Bidder does not demonstrate the Bidder's ability to recover its own costs in providing the relevant resource, Canada may declare the bid non-compliant, if the rate is at least **20%** of or lower than the median price bid by compliant bidders for the first year of the resulting contract for the relevant resource(s). Only the Firm Per Diem Rates of proposals that are technically responsive will be considered.

4.4 Supply Chain Integrity Process

a. During the RFP process, the Contract period and any resulting Option periods, the Supply Chain Security Authority identified by Canada, may, based on its National Security mandate to protect Canada's IT infrastructure as well as to assess threats, risks and vulnerabilities, assess the Bidder's SCSI.

b. Canada will assess whether, in its opinion, the Bidder's supply chain creates the possibility that the Bidder's supply chain or proposed solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information, or represents a threat to Canada's National Security, in accordance with Section 2.4 of Appendix H - Supply Chain Integrity Process.

It is a condition precedent to any contract award that a Bidder successfully satisfy the Security Authority's Supply Chain Integrity assessment.

4.5 Basis of Selection - Highest Combined Rating of Technical Merit and Price

4.5.1 To be declared responsive, a bid must:

a) comply with all the requirements of the bid solicitation;
b) meet all mandatory criteria; and
c) obtain the required minimum of **1459** points overall for the technical evaluation criteria which are subject to point rating.

The rating is performed on a scale of **2209** points.

4.5.1.2 Bids not meeting (a) or (b) or (c) will be declared non-responsive.

4.5.1.3 The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70% for the technical merit and 30% for the price.

4.5.1.4 To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70%.

4.5.1.5 To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30%.

4.5.1.6 For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

4.5.1.7 Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively. The total available points equal's 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating of Technical Merit (70%) and Price (30%)

		Bidder 1	Bidder 2	Bidder 3
Overall Technical Score		**115/135**	**89/135**	**92/135**
		$55,000.00	**$50,000.00**	**$45,000.00**
Calculations	**Technical Merit Score**	**115/135 x 70 = 59.63**	**89/135 x 70 = 46.15**	**92/135 x 70 = 47.70**
	Pricing Score	**45/55 x 30 = 24.55**	**45/50 x 30 = 27.00**	**45/45 x 30 = 30.00**
Combined rating		**84.18**	**73.15**	**77.70**
Overall rating		**1st**	**3rd**	**2nd**

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default, if any certification made by the Bidder is found to be untrue whether during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms for the Integrity Regime website, to be given further consideration in the procurement process.

5.1.2 Additional Certifications required with the bid

The following additional certification documents are required as part of the bid:

1. Form 1 – Software as a Service Publisher Certification Form
2. Form 2 – Software as a Service Publisher Authorization Form
3. Form 3 – SCSI Vendor Submission Form
4. Form 4 - Cloud SaaS Technical SCI Assessment controls Supplier Questionnaire

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy, the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Integrity Provisions – List of Names

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide a completed List of Names in the Integrity Verification form available on the Integrity Regime website, to be given further consideration in the procurement process.

5.2.3 Federal Contractors Program for Employment Equity – Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the webpage.

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the “FCP Limited Eligibility” to Bid list at the time of contract award.

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the “FCP Limited Eligibility to Bid” list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act*.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

Certification

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

PART 6 – SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

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

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

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

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

d) The bidder must complete the **Contract Security Program Application for Registration (AFR) for Canadian Legal** entities located in Appendix O and include a signed copy in their bid submission.

e) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

f) the Bidder must provide the address of the proposed site (s) for carrying out the work and saving documents, as indicated below:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

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

6.2 Insurance

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

PART 7 - RESULTING CONTRACT CLAUSES

APPENDIX A, GENERAL TERMS AND CONDITIONS

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

A1. Standard Acquisition Clauses and Conditions Manual

All instructions, general terms, conditions and clauses identified herein by title, number and date are set out in the Standard Acquisition Clauses and Conditions (SACC) Manual issued by Public Works and Government Services Canada (PWGSC) and in the Citizenship and Immigration Canada Terms and Conditions Manual.

A1.1 An electronic version of the SACC Manual is available on the Buy and Sell Website.

A1.2 An electronic version of the Immigration, Refugees and Citizenship Canada (IRCC) Contract Terms and Conditions is available on the IRCC Website.

A2. Terms and Conditions of the Contract

A2.1 The general terms, conditions and clauses identified herein by title, number and date, are hereby incorporated by reference into and form part of this Contract, as though expressly set out herein, subject to any other express terms and conditions herein contained.

A3. General Conditions

A3.1 General Conditions CIC-GC-001 (2020-12-02), Med/High Complexity Goods and Services Contract shall apply to and form part of this Contract.

APPENDIX "B", SUPPLEMENTAL TERMS AND CONDITIONS

B1. Priority of Documents

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

a) The Articles of Agreement;
b) Appendix B – Supplemental Terms and Conditions;
c) Appendix A – General Terms and Conditions;
d) Appendix D - Statement of Work
e) Annex A to Appendix D – Statement of Requirements
f) Appendix C - Terms of Payment – Task Authorizations;
g) Appendix E - Basis of Payment
h) Appendix G - Security and Privacy Obligations;
i) Appendix L - Tier 1 Security Requirements;
j) Appendix F - Security Requirements Checklist (SRCL);
k) Appendix H - Supply Chain Integrity Process
l) Appendix J - Service Level Agreement (SLA);
m) Appendix K - Non-Disclosure Agreement; and
n) The Contractor's proposal dated _____*(to be inserted at contract award)*

B2. CIC Clauses

The following Citizenship and Immigration Canada Terms and Conditions are incorporated by reference and form part of this Contract:

ID	Date	Title
CIC-SC-001(2015-02-16), Contractor Owns Intellectual Property (IP) Rights in Foreground Information		

B3. SACC Manual Clauses

The following SACC manual Clauses are incorporated by reference and form part of this Contract:

ID	Date	Title
A9117C	***2007-11-30***	***T1204 - Direct Request by Customer Department***
A9116C	***2007-11-30***	***T1204 Information Reporting by Contractor***

B4. Security Requirement

The security requirements (SRCL – Appendix F) and related clauses (Annex A to Appendix F), provided by the Contract Security Program and Appendix G, schedule 1 apply to and form part of the Contract.

B5. Period of Contract and Auto Renewal

Contract Period. The Contract Period includes the entire period of time during which the Contractor is obliged to provide the Services and perform the Work.

Initial Term. This Contract begins on the date the Contract is awarded and ends three (3) years later.

B5.1 Option to Extend the Contract.

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to three (3) additional 1-year periods under the same terms and conditions The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment. Canada may exercise the options at any time by sending a written notice to the Contractor at least

ten (10) calendar days before the expiry date of the Contract. The option may be exercised only by the Contracting Authority, and will be evidenced, for administrative purposes only, through an amendment to the Contract.

B5.2 Option to increase the level of effort

The Contractor grants to Canada the irrevocable option(s) to increase the level of effort of the Contract as per Appendix "E", Basis of Payment within the contract period under the same terms and conditions. The Contractor agrees that, during the options of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least ten (10) calendar days before the Contract expiry date. The option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

B5.3 Change in Consumption

The Contractor grants to Canada the irrevocable option to increase their consumption of the SaaS products or services detailed in Appendix D. Where Canada's consumption of the SaaS products or services is decreased, the Contractor agrees that no penalties or increase in pricing per unit shall apply as a result.

B5.4 Auto-Renewal Opt Out.

Canada hereby provides notice to the Contractor that it opts out of any auto-renewal of the term obligation. The Contractor acknowledges receipt of the notice, and represents that this Contract will be valid only until the end of the Contract Period, as defined above.

B6. Termination for Convenience

(a) Notice of Termination: The contracting Authority may serve the Contractor with written Notice of Termination for Convenience of part or all of the Contract. The Notice will identify the effective date of termination, the affected Work or Services (if partial termination), and any required Transition or Migration Services. The Contractor must comply with the requirements of the Notice, including continuing to perform or deliver Services or Work not affected by the termination.

(b) The Contractor agrees to immediately repay the portion of any advance payment that is unliquidated at the date of the termination to Canada.

(c) If, under (a) Canada terminates:

a. **Work**. Canada will pay the Contractor reasonable costs incidental to the termination of Work incurred by the Contractor, specifically excluding costs related to severance of employees, unless the Contractor establishes those costs arise from statutory obligations.

b. **Services**

i. For subscription Services paid monthly in advance, Canada will forego its right to claim the unliquidated portion of an advance payment at the date of termination; and

ii. For services on annual subscriptions or with defined Contract Periods, with annual advance payments, Canada will forego its right to claim that part of the portion of an advance payment that is unliquidated at the last day of the contract year following date of the termination.

(d). The parties agree that these amounts represent a genuine estimate of liquidated damages that would result to the Contractor for early termination of the Contract, and not a penalty.

B7. Certifications / Compliance and Additional Information

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are

conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

B7.1 Federal Contractors Program for Employment Equity - Default by the Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

B8. Insurance Requirements

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

B9. Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work in Appendix D.

B10. Authorities

<The Authorities for the Contract are to be identified at Contract award>

B10.1 Contracting Authority

The Contracting Authority for the Contract is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address:

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

B10.2 Project Authority

The Project Authority for the Contract is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address:

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has

no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

B10.3 Technical Authority

The Technical Authority for the Contract is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address

The Technical Authority will be responsible for providing guidance on the technical requirements and deliverables.

B10.4 Client Administrative Contact

The Client Administrative Contact is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address:

The Client Administrative Contact must receive the original Invoice. All inquiries for request for payment must be made to the Client Administrative Contact.

B10.5 Supply Chain Security Authority

Name:

Title:

Organization:

Address:

Telephone:

Email Address:

The Supply Chain Security Authority is the IRCC representative and is responsible for all matters concerning the ongoing Supply Chain Integrity Process under the Contract. Neither the Contracting Authority nor the Technical Authority have any authority to advise or authorize any information in relation to the Supply Chain Integrity Process. All other security-related matters remain the responsibility of the Supply Chain Security Authority.

B10.6 Contractor's Representative

The Contractor's Representative is:

Name:
Title:

Telephone:
Facsimile:
E-mail address:

B11. Proactive Disclosure of Contract with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

B12. Requirement

B12.1. The Contractor agrees to provide the Services and perform the Work described in the Contract in accordance with Appendix A – Statement of Work and at the prices set out in Appendix E – Basis of Payment. **Any pricing information included elsewhere in the Contract, including in Appendix J – SaaS Solution Service Level Agreement shall be deemed stricken and is of no force or effect.**

B12.2 Services. The Contractor agrees to provide the Services identified in Appendix D, which includes, at a minimum:

a. granting usage rights to the Software as a Service (SaaS) Solutions ("Solution(s)") identified in Appendix D provided by or hosted by the Contractor;
b. providing Solution Documentation;
c. maintaining, upgrading, and updating the Solution(s);
d. managing incidents and defects to ensure the Solution(s) operate at the applicable service levels;
e. providing incidental and additionally required information technology infrastructure services.
f. Providing infrastructure services required to deliver the Solution; and
g. Providing professional services and training, as and when requested by Canada

B12.3 Professional Services. The Contractor agrees to provide the following Professional Services, as and when requested by Canada, using the Task Authorization process:

a. Quick Start Guide ("QSG") training and services package;
b. implementation services;
c. training services;
d. data cleansing, migration and transition services; and
e. advisory services.

B12.4 Client. Under the Contract, the "Client" is Citizenship and Immigration Canada, hereinafter known as Immigration, Refugees and Citizenship Canada (IRCC).

B12.5 Reorganization of Clients. The Contractor's obligation to provide the Services and perform the Work will not be affected by (and no additional fees will be payable as a result of) any form of reorganization or restructuring of any Client. Canada may designate replacement Contracting Authority or Technical Authority.

B13. Solution

B13.1 Software as a Service. The Contractor will deliver the Solution through a Software as a Service ("SaaS") delivery model, allowing Canada to access and use the Solution which is hosted by the Contractor.

B13.2 Commercially-Available Solution. Canada acknowledges that the Solution is a commercially-available solution provided to other customers. As part of the subscription to use the Solution, the Contractor agrees to make available to Canada all the features and functionalities included in the commercially available version of the Solution, and the incidental and required information technology infrastructure services required to deliver the Solution, all of which is included in the subscription price.

B13.3 Software Application Evolution; Features or Functionalities. Canada acknowledges that the Solution, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the Services as the commercially available Solution, with functionality or features and on with terms that are no less favourable than as at the time of Contract award.

B13.4 Improvements to and Evolution of the Solution. The parties acknowledge that technology and business models evolve quickly and that any Solution provided at the beginning of the Contract Period inevitably will be different from the Solution provided at the end of the Contract Period and the method(s) by which the Solution and any potential peripherals are delivered to Canada are likely to change or evolve and that, at the time of entering into this Contract, the parties cannot possibly contemplate all the goods or services that may be delivered under this Contract, other than they will be connected to delivering to Users. With that in mind, the parties agree that:

a) The Contractor must maintain and continuously improve the Solution and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide those improvements and enhancements to Canada as part of Canada's subscription, with no price adjustment if those improvements and enhancements are also offered to other customers at no additional cost.

b) If the Contractor removes any functions from the commercial offering to the Solution and offers those functions in any new or other services or products, the Contractor must continue to provide those functions to Canada as part of Canada's subscription to the Services, under the existing terms and conditions of the Contract regardless of whether those other services or products also contain new or additional functions. Contractor has no obligation to comply with this paragraph if the Solution acquired by Canada is still offered by Contractor in parallel with the new services offered to other customers.

B13.5 Downgrade. If the Contractor is unable to provide the Services with no less favourable features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract, and pay all identifiable direct costs incurred by Canada to migrate and store Client's Data, and to procure equivalent replacement services.

B14. Services

B14.1 Solution Services

(a) **Software as a Service.** The Contractor will provide all Services required for Canada to access and use the Solution as specified in Appendix D – Statement of Work and Annex A to Appendix D Statement of Requirements.

(b) **Authority.** The Contractor represents and warrants that it owns or has obtained and will maintain throughout the Contract Period, all necessary authority specifically including intellectual property rights required to provide the Services in accordance with the terms of this Contract.

(c) **Remedies for an alleged breach of intellectual property.** If anyone claims that as a result of Canada's access or use of the SaaS Services, Canada is infringing its intellectual property rights, Canada will promptly notify the Supplier in writing about the claim. In the above circumstances, or if anyone claims that the Supplier is infringing its intellectual property rights in relation to the subject SaaS solution of this Contract.

The Supplier must immediately do one of the following:

(i) take all necessary steps to acquire the rights to be able to continue to provide Canada the Solution Services in accordance with the Contract;

(ii) modify or replace the allegedly infringing part of or the whole SaaS solution, and continue to provide Canada the Solution Services in accordance with the Contract;

(iii) if the above options are not viable, the Supplier agrees to provide written notice of the claim to Canada, and propose an alternate "Replacement" SaaS solution as a new or interim basis of the Solution Services under this Contract. The Supplier agrees to provide the new or interim Solution Services at the same price as the subject Solution Services, for the duration of the Contract Period, regardless of the Supplier's commercial price for the Replacement SaaS solution, or whether the Replacement SaaS solution has greater functionality. Additionally, the Supplier agrees to provide training at no additional cost if required by Canada for its use of the Replacement SaaS Solution.

(iv) provide written notice to Canada to terminate the Contract, including the name of the claimant, the nature of the claim, the Supplier's purported authority to the allegedly infringing part of the SaaS solution and a confirmation of the Supplier's inability to continue to provide Canada the Solution Services in accordance with the Contract. For this termination right, the Supplier agrees to provide Canada extended access to any GC data used or stored through the SaaS solution for recovery or migration, and agrees to fully refund any part of the Contract Price that Canada has already paid in previous 12 months, or from the date of infringement, whichever is earlier.

If the supplier fails to comply with this section within a reasonable amount of time, the Supplier agrees to reimburse Canada for all the costs Canada may incur to resolve the infringement claim, including the procurement of new Solutions Services

(d) **Accessibility:** The Contractor must ensure that the Solution does not interfere with accessibility standards compliance, as specified in the Standard on Web Accessibility: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601#

(e) **Usage Grant**. The Contractor grants to Canada the non-exclusive, non-assignable right to access and use the Solution from an unlimited number of locations, devices and operating environments, through secure, wireless, mobile or other connection, via the internet, a web browser or other access connection technology which may become available.

(f) **Included.** The Contractor represents and warrants that the Services include:

i. hosting and maintenance of the Solution
ii. Provision of all incidental and additional required information technology infrastructure services in compliance with all required security standards
iii. the technical infrastructure that complies with all required security standards, allowing Canada to use the Solution to process any of Client's Data in compliance with its expressed security standards, and
iv. unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Solution,

all of which is included in the price.

(g) **Restricted Usage Rights.** Canada acknowledges that in providing the Services, the Contractor is not delivering ownership rights to any software product, component of the Solution or infrastructure used by the Contractor to provide the Services, except as expressly provided in a Task Authorization. Canada will not knowingly:

a. distribute, license, loan, or sell the Solution;
b. impair or circumvent the Solution's security mechanisms; or

c. remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Solution.

(h) **Applicable Terms and Conditions**. The Contractor has advised and Canada acknowledges that the Contractor may unilaterally modify the terms under which it provides its commercial offering of the Solution, without notice to its customers, including Canada. The Contactor represents and warrants that any such modification will not result in less favourable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

(i) **Additional Terms and Conditions.** The parties agree that any terms and conditions, including any "click-through" or "pop-up" notices, that apply to the Contractor's commercial offering of the Solution, including third party tools or incidental infrastructure, will not apply to Canada's use of the Solution if those terms conflict with the express terms of this Contract. The terms and conditions of third party tools not specified as a Service or Solution in Appendix D are not subject to this section.

(j) **Commercial SaaS Offering.** Canada acknowledges that it will accept the Contractor's commercial SaaS offering, and states that, unless explicitly identified as Work or Services to be delivered under this Contract, Canada does not require custom development, alternative services, service levels, functionalities or features.

(k) **Data Retrieval:** The Contractor agrees to make Canada's data available for a minimum of 90 days after the end of the Contract to allow the Client sufficient time to migrate their data to a new environment, at no additional cost to Canada.

(l) **Application Programming Interfaces (API)**

The Contractor must:

i. Provide services that use open, published, supported, and documented Application Programming Interfaces (API) to support activities such as interoperability between components and to facilitate migration of applications; and,
ii. Provide a means via API for applications to provision services, and extract reporting, billing and financial data pertaining to the cloud services consumed by the Client.
iii. Take reasonable measures to protect both internal and external APIs through secure authentication methods. This includes ensuring that all externally exposed API queries require successful authentication before they can be called and providing the ability for the GC to meet the GC's standards on API (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html).

B15. Service Levels

Appendix J Service Level Agreement (provided by the Contractor) contains the specific information defining the levels and standards for processes and performance expectations for the Services to be delivered under the Contract, and must be read in conjunction with the following section.

B15.1. Availability. The Contractor will make the Service available to Canada in strict compliance with Solution Documentation and Appendix J, Service Level Agreement.

B15.2 Service Credits. The Contractor will provide the applicable Service Credits to Canada for failing to achieve the uptime Solution Availability levels as defined in Appendix J, Service Level Agreement.

B15.3 Exclusions. The Contractor will expressly specify any exclusions to the Solution Availability levels identified in Appendix J, Service Level Agreement.

B15.4 Support Services. The Contractor will provide technical support assistance in strict compliance with Appendix J, Service Level Agreement.

B15.5 Escalation. The Contractor will provide an escalation process for dispute resolution, which is identified in Appendix J, Service Level Agreement.

B15.6 No Infringement. The Contractor warrants that nothing in the Solution, or in Canada's use of the Solution, will infringe or constitute a misappropriation of the intellectual property or other rights of a third party.

B16. Service Level Agreements

B16.1. The Contractor's Published SaaS Service Level Agreement is attached in Appendix J. The service level commitments (detailed in Appendix J) must provide commercial client support which includes, at the minimum, any published and commercially available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the SaaS Solution.

B16.2 The following terms must be addressed in the Appendix J SLA:

A. period during which the Contractor will provide warranty and support;
B. contact and procedure information for accessing support;
C. procedures for resolution of problems;
D. response times;
E. procedures on how and when all telephone, fax or email communications will be responded to;
F. website support availability to Clients (e.g. 24 hours a day, 365 days a year, and 99.9% of the time); and
G. Maintenance entitlements (e.g. patches, updates, major/minor releases,

B16.3 Notifications Required for Tier 1 (Protected A) and Tier 2 (Protected B) requirements.

The Contractor must provide the following:

b) Notification of any interruption that is expected to impact service availability and performance, as agreed to by the parties and included in the Service Level Agreements (SLAs);

c) Regular updates on the status of returning the services to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-implementation alerts;

d) Notification for services that will be discontinued and that has an impact on customer Services;

Any terms contained in Appendix J that purport to interpret the Contract, are the same or similar subject matter, or are related to the terms contained in Contract, are deemed stricken and are of no force or effect.

B17. Documentation

B17.1 Solution Documentation. The Contractor must provide or deliver access to the commercially available Solution Documentation to Canada upon Contract Award. The Contractor must update Solution Documentation on a commercially reasonable basis**.**

B17.2 Other Documentation. The Contractor must provide or deliver access to any documentation required in performance of the Work.

B17.3 Translation Rights. The Contractor agrees that Canada may translate any written deliverable, including the Solution Documentation or Training Materials into English or French. The Contractor acknowledges that Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor will not be responsible for technical errors that arise as a result of any translation made by Canada.

B17.4 Moral Rights. At the request of Canada, the Contractor may provide a written permanent waiver of moral rights, in a form acceptable to Canada, from every author that contributed to the written deliverable. If the

Contractor is unable or unwilling to obtain the requested waivers, the Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any moral rights infringement claim by a third party based on Canada's translation of written documentation.

B17.5 Defective Documentation. If at any time during the Contract Period, Canada advises the Contractor of a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor must correct the defect or non-conformance as soon as possible and at its own expense. Canada may provide the Contractor with information about defects or non-conformance in other documentation, including the Solution Documentation, for information purposes only.

B18. Work

18.1 Professional Services

(a) **Professional Services.** The Contractor must perform and deliver such Professional Services (the "Work") to Canada as detailed in a Task Authorization.

B18.2 Remedies

(a) **Work.** If at any time during the Contract Period the Work fails to meet its warranty obligations, the Contractor must as soon as possible correct at its own expense any errors or defects and make any necessary changes to the Work.

(b) **Canada's Right to Remedy.** If the Contractor fails to fulfill any obligation described herein within a reasonable time of receiving a notice, Canada will have the right to remedy or to have remedied the defective or non-conforming Work at the Contractor's expense. If Canada does not wish to correct or replace the defective or non-conforming Work, an equitable reduction will be made in the Contract Price.

B18.3 Excusable Delay

Subsection A11 Excusable Delay of CIC-GC-001 – 2020-12-02 General Terms and Conditions – Medium/High Complexity Goods and Services Contracts, is amended as follows:

Add:

Right to Terminate

If such an event prevents performance under the Contract for more than 30 calendar days, then the Contracting Authority may elect to terminate the TA, or part or all of this Contract on a "no fault" basis, meaning neither party will be liable to the other in connection with the Excusable Delay or resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

B18.4 Professional Services: Transition Services

(a) **Migration.** The Contractor acknowledges that the nature of the Services provided under the Contract, Canada may require continuity. Prior to the transition to the new contractor or to Canada, the Contactor must provide all operational, technical, design and configuration information and documentation for all Services required to complete the transition, provided that it is not Contractor confidential information. The Contractor represents and warrants that it will not directly or indirectly interfere with or impede Canada's access to or transfer of Client's Data.

(b) **Migration and Transition Services.** The Contractor agrees that, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, it will diligently assist Canada in the transition from the Contract to a new contract with another supplier and or migrate Client's Data to a new supplier environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment.

B18.5 Inspection and Acceptance of the Work

Subsection A12 Inspection and Acceptance of the Work of CIC-GC-001 – 2020-12-02 General Terms and Conditions – Medium/High Complexity Goods and Services Contracts, is amended as follow:

Add:

(a) **Acceptance Procedures**: Unless provided otherwise in the Contract, the acceptance procedures are as follows:

(i) when the Work is complete, the Contractor must notify the Technical Authority in writing, with a copy to the Contracting Authority, by referring to this provision of the Contract and requesting acceptance of the Work;

(ii) Canada will have 30 days from receipt of the notice to perform its inspection (the **"Acceptance Period**").

(b) **Deficiencies and Resubmission of Deliverable**: If Canada provides notice of a deficiency during the Acceptance Period, the Contractor must address the deficiency as soon as possible and notify Canada in writing once the Work is complete, at which time Canada will be entitled to re-inspect the Work before acceptance and the Acceptance Period will begin again. If Canada determines that a deliverable is incomplete or deficient, Canada is not required to identify all missing items or all deficiencies before rejecting the deliverable.

(c) **Access to Locations**: The Contractor must provide representatives of Canada access to all locations where any part of the Work is being performed, other than multi-tenant data centres, at any time during working hours. Representatives of Canada may make examinations and such tests of the Work as they may think fit. The Contractor must provide all assistance and facilities, test pieces, samples and documentation that the representatives of Canada may reasonably require for the carrying out of the inspection. The Contractor must forward such test pieces and samples to such person or location as Canada specifies.

(d) **Contractor Inspection for Quality**: The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to Canada. All deliverables submitted by the Contractor must be of a professional quality, free of typographical and other errors, and consistent with the highest industry standards.

(e) **Inspection Records**: The Contractor must keep accurate and complete inspection records that must be made available to Canada on request. Representatives of Canada may make copies and take extracts of the records during the performance of the Contract and for up to three years after the end of the Contract.

(f) **Informal Feedback**: Upon request by the Contractor, Canada may provide informal feedback prior to any deliverable being formally submitted for acceptance. However, this must not be used as a form of quality control for the Contractor's Work. Canada is not obliged to provide informal feedback.

B19. Basis of Payment

B19.1 Subscription. For the Services, including access to and use of the Solution, Solution Documentation, Support Services, and incidental and additionally required information technology infrastructure services (all the Services described in this Contract that is not Work), Canada shall pay the prices detailed in Appendix E – Basis of Payment.

B19.2 Professional Services provided under a Task Authorization: For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables / the firm price set out in the Task Authorization, in accordance with the firm all-inclusive per diem rates set out in Appendix E, Basis of Payment or in the Contractors bid, as applicable. Applicable Taxes extra.

B19.3 On-Site Support Charges. If approved in advance by Canada, the Contractor will be paid the hourly or daily labour rates specified in the Contract, together with reasonable and proper travel and living costs incurred by the Contractor in connection with on-site services. Any travel and living costs will only be reimbursed in accordance with the applicable meal and private vehicle allowances provided in the National Joint Council Travel Directive, as amended from time to time. All such pre-approved costs must be invoiced to Canada as a separate charge.

B19.4 Pricing Stability

The Contractor acknowledges that it is important to Canada to be able to continue to access the SaaS products and services detailed in Appendix D – Statement of Work after the Term of Contract. The Contractor accordingly offers to continue to provide the SaaS products and services at reasonable rates and on all of the other terms and conditions set out in this Contract, subject to execution by the parties of a formal contract(s) therefor. For each of the 2 years that follow the Term of Contract, the Contractor hereby offers annual rates that are the lesser of:

(a) the Contractor's then current published rates; and

(b) the previously contracted rates adjusted by the percentage difference in the Consumer Price Index (CPI) as determined by Statistics Canada, for the 12 month period immediately preceding the date on which the price change is to be effective; and

(c) 3% more than the annual rates provided to Canada in the preceding year under this Contract or under any extension entered into pursuant to this Article;

and the Contractor's obligations under this Article shall survive termination or expiry of this Contract.

B19.5 Price Certification

The Contractor certifies that the price quoted is not in excess of the lowest price charged anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both.

B19.6 Discretionary Audit

The Contractor's certification that the price or rate is not in excess of the lowest price or rate charged to anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both, is subject to verification by government audit, at the discretion of Canada, before or after payment is made to the Contractor.

If the audit demonstrates that the certification is in error after payment is made to the Contractor, the Contractor must, at the discretion of Canada, make repayment to Canada in the amount found to be in excess of the lowest price or rate or authorize the retention by Canada of that amount by way of deduction from any sum of money that may be due or payable to the Contractor pursuant to the Contract.

If the audit demonstrates that the certification is in error before payment is made, the Contractor agrees that any pending invoice will be adjusted by Canada in accordance with the results of the audit. It is further agreed that if the Contract is still in effect at the time of the verification, the price or rate will be lowered in accordance with the results of the audit.

B20. Payments

B20.1 Invoices

Subsection A13 Invoice Submission of CIC-GC-001 – (2020-12-02) General Terms and Conditions – Medium/High Complexity Goods and Services Contracts, is amended as follows:

Add:

Withholding for Non-Residents. Canada must withhold 15 percent of the amount to be paid to the Contractor in respect of services provided in Canada if the Contractor is not a resident of Canada, unless the Contractor obtains a valid waiver from the Canada Revenue Agency. The amount withheld will be held on account for the Contractor in respect to any tax liability which may be owed to Canada.

B20.2 Method of Payment

(a) Canada will make payment to the Contractor for the Services either in advance or in arrears, in accordance with Appendix C – Terms of Payment. Where payment is made in advance, the advance payment period shall not exceed 12 months. Payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or the delivery of the Services.

(b) If Canada disputes an invoice for any reason, Canada will pay the Contractor the undisputed portion of the invoice, as long as the undisputed items are separate line items on the invoice and owed. In the case of disputed invoices, the invoice will only be considered to have been received for the purposes of section A18 of CIC-GC-001 – (2020-12-02) General Terms and Conditions – Medium/High Complexity Goods and Services Contracts, article 3 once the dispute is resolved.

B20.3 Limitation of Expenditure. Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

B20.4 Electronic Payment of Invoices. The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

(a) Visa Acquisition Card:
(b) MasterCard Acquisition Card;
(c) Direct Deposit (Domestic and International);
(d) Electronic Data Interchange (EDI);
(e) Wire Transfer (International Only);
(f) Large Value Transfer System (LVTS) (Over $25M)

B21. Limitation of Liability – Information management/Information Technology

1. This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this section, even if it has been made aware of the potential for those damages.

2. First Party Liability:

   a. The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

i. any infringement of intellectual property rights to the extent the Contractor breaches the section of the general conditions entitled "Intellectual Property Infringement and Royalties";

ii. physical injury, including death.

b. The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

c. Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

d. The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (a) above.

e. The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

i. any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including Applicable Taxes) for the goods and services affected by the breach of warranty; and

ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of 0.25 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1,000,000.00 .

In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the Contract or $1,000,000.00.

f. If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

3. Third Party Claims:

a. Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the

damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

b. If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph (a), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

c. The Parties are only liable to one another for damages to third parties to the extent described in this paragraph 3.

B22. General Provisions

Subsection A28 Amendments and Waivers of CIC-GC-001 – (2020-12-02) General Terms and Conditions – Medium/High Complexity Goods and Services Contracts, is amended as follows:

Add:

Waiver. The failure or neglect by a party to enforce any of the rights under this Contract will not be deemed to be a waiver of that party's rights.

APPENDIX C, TERMS OF PAYMENT
TASK AUTHORIZATIONS

C1. Basis of Payment

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid firm unit prices as specified in Appendix E – Basis of Payment for a cost of $_____ (*to be added at contract award*). Customs duties are included and applicable taxes are extra.

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

C2. Task Authorization:

The Work or a portion of the Work to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract.

C2.1 Task Authorization Process:

1. The Technical Authority will provide the Contractor with a description of the task using the "Task Authorization Form specified in Appendix I.
2. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis (bases) and methods of payment as specified in the Contract.
3. The Contractor must provide the Technical Authority, within 2 business days of its receipt, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract.
4. The Contractor must not commence work until a TA authorized by the Contracting Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

C2.2 Canada's Obligation – Portion of the Work - Task Authorizations:

Canada's obligation with respect to the portion of the Work under the Contract that is performed through task authorizations is limited to the total amount of the actual tasks performed by the Contractor.

C2.3 Periodic Usage Reports – Contracts with Task Authorizations:

The Contractor must compile and maintain records on its provision of services to the federal government under authorized Task Authorizations issued under the Contract.

The Contractor must provide this data in accordance with the reporting requirements detailed in Appendix M. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "NIL" report.

The data must be submitted on a quarterly to the Contracting Authority.

The quarterly periods are defined as follows:
1st quarter: April 1 to June 30;
2nd quarter: July 1 to September 30;
3rd quarter: October 1 to December 31; and
4th quarter: January 1 to March 31.
The data must be submitted to the Contracting Authority no later than 10 calendar days after the end of the reporting period.

Reporting Requirement- Details:

A detailed and current record of all authorized tasks must be kept for each contract with a task authorization process. This record must contain

For each authorized task:

i. the authorized task number or task revision number(s);
ii. a title or a brief description of each authorized task;
iii. the total estimated cost specified in the authorized Task Authorization (TA) of each task, applicable taxes extra;
iv. the total amount, applicable taxes extra, expended to date against each authorized task;
v. the start and completion date for each authorized task; and
vi. the active status of each authorized task, as applicable.

For all authorized tasks:

i. the amount (applicable taxes extra) specified in the contract (as last amended, as applicable) as Canada's total liability to the contractor for all authorized TAs; and
ii. the total amount, applicable taxes extra, expended to date against all authorized TA's.

C3. Basis of Payment – Task Authorization

For professional services requested by Canada, in accordance with an approved Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in Appendix E, Basis of Payment, applicable taxes extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.

C3.1. Limitation of Expenditure

1. Canada's total liability to the Contractor under the Contract must not exceed $ _____. Customs duties are included and applicable taxes are extra.
2. No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:
    a. when it is 75 percent committed, or
    b. four (4) months before the contract expiry date, or
    c. as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

    whichever comes first.
3. If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

C4. Method of Payment

C4.1 Onboarding Fee (one-time fee)

Canada will pay the Contractor upon completion and delivery of the Set-up and Configuration, and the training in accordance with the payment provisions of the Contract if:

a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b) all such documents have been verified by Canada;
c) the Work delivered has been accepted by Canada.

C4.2 Annual Subscription Fee and Professional Services

Canada will pay the Contractor on a yearly basis for work performed during the year covered by the invoice in accordance with the payment provisions of the Contract if:

a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b) all such documents have been verified by Canada;
c) the Work performed has been accepted by Canada.

Canada will make payment to the Contract for the Services either in advance or in arrears, in accordance with Appendix J Service Level Agreement or the Contractor's bid, as applicable. Where payment is made in advance, the advance payment period shall not exceed 12 months. Payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or the delivery of the Services.

If Canada disputes an invoice for any reason, Canada will pay the Contractor the undisputed portion of the invoice, as long as the undisputed items are separate line items on the invoice and owed. In the case of disputed invoices, the invoice will only be considered to have been received for the purposes of the section A18 Interest on Overdue Accounts once the dispute is resolved.

For each individual Task Authorization issued under the Contract that contains a maximum price:

a. Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice;
b. Once Canada has paid the maximum price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the Task Authorization, all of which is required to be performed for the maximum price. If the work described in the Task Authorization is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum price, Canada is only required to pay for the time spent performing the work related to that Task Authorization/Contract.

C5. Applicable Taxes

Applicable taxes are not included in the amounts shown in the Basis of Payment. Applicable taxes, which are estimated at $_____ *(to be determined at contract award)*, are included in the total contract amount. Applicable taxes are to be shown as separate items on all invoices and claims for progress payments and will be paid by Canada. The Contractor agrees to remit to appropriate tax authorities any amounts of Applicable Taxes paid or due.

C6. Invoicing Instructions

1. The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.
   Each invoice must be supported by:
   a. a copy of time sheets to support the time claimed;
   b. a copy of the release document and any other documents as specified in the Contract;

2. Invoices must be distributed as follows:

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

C7. Travel and Living Expenses

Canada will not accept any travel and living expenses outside of those outlined in B.19.3 Onsite Support charges, for:

a) Work performed within the National Capital Region (NCR). The NCR is defined in the National Capital Act, R.S.C. 1985, c. N-4, S.2.;
b) Any travel between the Contractor's place of business and the NCR; and
c) Any relocation of resources required to satisfy the terms of the Contract.

These expenses are included in the firm price for professional fees specified above.

APPENDIX D, STATEMENT OF WORK

D1. Title

Cloud based Enterprise Learning Management System (LMS) for department wide use at Immigration, Refugees and Citizenship Canada (IRCC).

D2. Objective

Immigration, Refugees and Citizenship Canada (IRCC) is seeking a contractor with a Software-as-a-Service (SaaS) application to host a solution that can be configured to meet specific IRCC requirements that allows for the management, delivery, tracking, reporting, and evaluation of all training and learning content.

The end state will be a cloud-based, browser accessed technology-enabled system, available to up to 15,000 departmental employees. This system will allow employees to consume learning content while maintaining and tracking their progress. The cloud-based application/system must provide a streamlined and enhanced end-to-end learning experience and allow effective, complete, and overall control of learning content management, robust analytics, administration, and communication with learners, learning providers, and decision makers.

D3. Background

The Enterprise Change & Learning Academy Branch (ECLA) has the functional authority for learning in IRCC, and as that authority, is looking to put in place a department wide Learning Management System (herein known as the LMS or the Solution) to standardize learning across the department. Growth in the Department is constant, resulting in a significant demand for training. Currently, a significant part of the training delivery function at IRCC is managed by the Learning Academy (LA) within ECLA.

Senior management has emphasized the need for timely reporting, monitoring and compliance of learning activities throughout the department. To ensure that the Learning and Development Division has the access and control to deliver on the new approved learning priorities at IRCC in a standardized way, a mandated department wide LMS is be the proposed solution.

An LMS will provide IRCC with a streamlined and enhanced end-to-end learning experience. It will allow effective, complete, and overall control of learning content management, administration, and communication with learners, learning providers, and decision makers. It will also be a powerful tool that can help IRCC align learning to business needs. An LMS will provide a single system of record for learning data coupled with accounting controls/tracking to allow for a fulsome understanding of IRCC's learning investment, and facilitate measurement of the value and impact of learning on individual and organizational performance. Enhanced analytics provided by an LMS will allow IRCC to fully measure and report on all learning managed across the department.

D4. Scope of Work

The Contractor must provide an LMS that will give IRCC an enterprise system for end-to-end management of employee learning, and an integrated back office for learning content management, delivery, analytics, and reporting which complies with departmental requirements.

The scope of work includes the acquisition, configuration and implementation of a system that provides IRCC with the following elements and general functionalities:

a. a common repository of operational information for Learning Management System (LMS) that manages:

   i. Learner, Learning Product and Learning Object Catalogue, and Registration information;
   ii. Learner historical learning information;
   iii. Curriculum and Certification information; and

iv. Registers Learners to Programs or Learning Products through on-line registration, and registration through a central role or roles.

b. a common repository for Learning Products and Learning Objects

c. a common repository for logistics information, including:
   i. Classrooms;
   ii. Equipment; and
   iii. Course / offering related materials

d. a common repository or authoritative source of information from which reports will be generated for IRCC and departmental administrators and managers.

e. Remote access for Learners, administrators and IRCC management and administrators, within the National Capital Region (NCR) as well as all regions in Canada and if required, IRCC employees working abroad.

f. A method for IRCC to self-administer all administrative roles

D4.1 Key Components of the Work

The key objective and scope of this work will be the acquisition, configuration and operation of a Cloud-Based Learning Management System (LMS).

Key components of the work include:

a. The delivery of a fully functional, hosted, commercial-off-the-shelf (COTS) cloud based SaaS model LMS which is described in the statement of requirements (Annex A to Appendix D) and D4.2. The associated cost must include all of the subscription licenses for the LMS to be operational, fully functional and secure within the vendor provided Data Centre, while adhering to the cloud hosting security and intellectual property requirements identified by IRCC. The application must meet all the required security specifications as outlined in Section D7 – Limitations and Constraints.

b. The preparation, the setup and configuration of as well as the turn-over to IRCC of the LMS. The preparation work also includes technical and business consulting resources required to perform the actual configuration.

c. An LMS that must meet the Government of Canada Security Control profile for Cloud-Based GC Services. The guidelines are available here: *Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103)* https://cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103#annb

D4.2 Requirements

The Solution must include the functional requirements listed in Table A of Annex A to Appendix D - Statement of IRCC LMS Requirements and **must** also include the following additional mandatory functionality:

a. A cloud-based solution that is platform and device-agnostic, accessible by all users, including system administrators, without the need for any additional software installation.
b. All upgrades, including regulatory updates, are provided at no additional cost.

c. The Solution must scale to at least 25,000 Authorized Users and allow for scalability over the lifespan of the Contract.
d. Single sign-on integration support
e. Multiple SaaS environments (Development, Testing and Production) hosted in a secure data center environment located in Canada
f. Multi-tenancy configurations with granular access, individual branding and security
g. Must allow IRCC to configure and maintain the solution as required
h. All data processed, stored and maintained in the solution, including all online storage as well as data backups and archived data, must reside in Canada.
i. Product Roadmap and Releases - Based on previous product releases, the Contractor must demonstrate continuing product investment by having a minimum of two substantive product releases per year based on previous product releases.
    i. The Contractor must demonstrate the availability of a product roadmap.
    ii. The Contractor must demonstrate a process that defines how the user community can propose enhancements and new features and how and when product features are decided, prioritized, developed and released.

D4.3 Delivery

The Contractor must deliver, set up and configure the cloud LMS in Canada, and must install and configure in the solution in such a way that all data, including data backups remain within Canada. The LMS however will be accessed by End Users, both learners and administrators across Canada and around the world through the Internet.

D5. Tasks and Deliverables

The Contractor must be able to meet the following mandatory requirements and deliver the following items to the Client Technical Authority:

D5.1 Fully functional Solution

a. The successful implementation will require a disciplined approach that includes services for project management, system design configurations, deployment, documentation, testing, training and IRCC Administrator support. IRCC requires an implementation where the Contractor must configure and provide on-going support for the fully-functional Solution, including:

    i. Providing in-depth, as-and-when requested consultation regarding best practices and process efficiencies, ensuring a successful integration with IRCC's processes and procedures;
    ii. Providing as-and-when requested IRCC Administrator training and training materials for end users and administrators
    iii. Providing support to ensure that IRCC maximizes both the use and cost effectiveness of the Solution.

b. To ensure the success of the implementation of the Solution, it must include, at a minimum, the implementation deliverables listed below. The Contractor must create each deliverable and must formally present them to IRCC for review and acceptance. In instances where there are milestones with multiple stages or milestones with stages that are required as prerequisites to the following stage or stages, the stages must be fully detailed to contain each deliverable, (unless noted otherwise).

    The Contractor must provide the following implementation deliverables:

    a. One (1) fully-functional, hosted, cloud-based SaaS LMS with the ability to support digital learning and development for IRCC employees and includes:

i. An average of 5,000 monthly active users nationwide;
ii. All solution usage rights granted, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada.

b. Comprehensive Project Plan, including:
   i. Project Implementation Plan:
      - Detailed listing of Stages, tasks and subtasks for the entire Project that includes: start and completion dates, roles and associated responsibilities, and predecessors. Tasks include, but are not limited to, all implementation activity, deadlines, milestones, draft deliverables, review periods, final deliverables and sign offs.
   ii. Communication Plan:
      - Detailed processes of how communications and engagement will effectively occur between IRCC and vendor, including descriptions on points of contact, frequency, and methodologies.
   iii. Risk and Issues Management/Mitigation Plan:
      - Detailed process explains how any risks or issues, will be identified and tabled by either the vendor or IRCC and that are predetermined or arise throughout the project lifecycle.
   iv. On-Going Communication, Coordination and Project Status Reports
      - Reports to be created and delivered on an as-and-when requested basis
   v. Technical Infrastructure Design and Implementation Plan
      - Design for hosted environments proposed by the Contractor, containing, at a minimum information on:
         A. Methodology, tools, procedures, activities, and services
         B. Security infrastructure and services (identify, protective, monitoring/detective, and responsive/recovery)
         C. Network and connectivity
         D. Performance characteristics
         E. Availability and flexibility requirements.
   vi. System Design Blueprint
c. Work product that identifies both business process decisions as well as system configuration decisions for each in scope business process and system feature.
   i. System Configuration, Migration and Integration
      1. Configuration
      2. Data Migration (as required)
      3. Report Implementation and Development (as required)
      4. Application Integration
   ii. Testing
      1. Test Plans and Scripts (as required)
      2. User Acceptance Testing
      3. Pre-production security testing.
   iii. Training
      1. User training for end-users who will be accessing and administering the Solution.
   iv. System Administration documentation and training: complete system manual and quick reference aids for how to use the configured system.
   v. Support Plan
      - A support plan for ongoing maintenance support for the duration of the Contract.
   vi. Implementation Plan

- Complete set of activities required for Go-Live, including Go-Live and Post Go-Live Support.

D5.2 Professional Services

The Contractor must provide professional services, as and when requested, in accordance with the Task Authorization Process. Professional Services are for the pre-planning and start-up required to operationalize the LMS, as well as for training, and post contract award in relation to the LMS for use by IRCC. Task Authorizations will be used by the Technical Authority for any purpose within the Scope or context of this SOW to support IRCC's LMS up to the maximum value specified by the Technical Authority.

The following professional resources will be required in support of the configuration, migration, change management, etc. of IRCC's new LMS. The following list of activities are subject to change post contract award once the various activities are underway.

The Contractor must provide the following resource categories on an as-and-when requested basis. The tasks include but are not limited to the following activities:

List of Professional Services		
ID	**Role Title**	**Role Description**
P1	Project Manager	IRCC requires a Project Manager to manage the configuration and assist with the full migration exercise. This includes working to ensure that the install goes well, working with the stakeholders on a day to day basis on the migration. a. Organize and manage the project including establishing standards, developing an effective project plan for the installation, configuration and start-up of the LMS, manage any changes that may impact the project, and manage the project tasks; b. Implement project management processes and practices; c. Assist in the identification and resolution of Issues; d. Ensure the project meets its objectives; e. report on the project resource consumption; f. ensure deliverables are complete, produced to schedule and budget and meet the quality specified; g. Develop and/or implement a change management strategy; h. Develop and/or implement a risk management strategy;
P2	Business Analyst	A Business Analyst is required to develop and implement the actual processes. While business processes are fixed, IRCC has the need to have the processes documented in terms that IRCC staff is familiar with. This role includes working with the project manager and IRCC project team on plans to migrate from the current processes to the LMS solution. a. Define business processes, and recommend changes to system architecture, system configurations, and technical migration strategies; b. Work with the project manager to develop, estimate and manage the project plan; c. Identify critical milestones and ensure that they are included in the overall plan; d. Develop and Review process and learning documentation to ensure it is of suitable efficacy and quality; e. Prepare process and data migration plans; f. Assist in determining and implementing the security requirements; and g. Work with testing and training teams on technical, data and organizational Issues/requirements and their timing.

P3	Information Architect	This role has two responsibilities: 1. Working with stakeholders on initial migration (i.e., assemble and format data for migration) 2. Working with stakeholders on requirements and processes for integration of LMS and PeopleSoft data This role is intended to support both learner and transcript data and content. • Define processes for integration of relationship of LMS to other Enterprise systems (i.e. PeopleSoft) • Define data migration strategies; • Prepare technical and data conversion plans; • Work with the project manager to develop, estimate and manage the data aspects of the project plan; • Document Data Model designs and their changes; • Assist in the development of prototypes; • Assist in the testing processes; • Conduct operational Data Model QA verification and validation reviews
P4	Change Manager	This resource must help IRCC manage the implementation, adoption, and use of the new LMS Cloud system. a. Manage the process of implementing major changes brought about by the project to reduce the risks and costs of change, and to optimize its benefits. b. Provide the leadership and direction necessary for the project to succeed. c. Plan and strategize how the project can overcome resistance to change. Focus on the Issues of managing the resistance and discomfort experienced by Learners within IRCC who are impacted by the LMS project. d. Administer project initiated changes: e. Use tested methods and techniques in order to avoid new errors and minimize the impact of changes f. Complete set of processes to ensure that changes are implemented in a visible, controlled and orderly fashion. g. Undertake to systematically deal with the project impacts on organizational change. h. Define and instill new values, attitudes, norms, and behaviors within the context of the project and its impact on the organization that provides new ways of doing work and overcome resistance to change. i. Build consensus among learners and stakeholders on specific changes designed to better meet their needs. j. Plan, test, and implement all aspects of the transition carried forward by the project, into the organization.
P5	Trainer	The Contractor must propose qualified training staff for both learners and administrators to: a. Develop and/or implement a training strategy and approach, in consultation with the Technical Authority or authorized designate; b. Monitor and assess training needs; c. Develop methodologies, and create/maintain training packages; d. Deliver training; e. Monitor effectiveness of training; f. Document strategies, methods and training packages; g. Work with the Technical Authority to develop, estimate and manage the training aspects of the LMS; and: h. Provide advice to the Technical Authority or authorized designate.

		i. The Trainer must perform the above in either French or English, as determined by the Technical Authority and specified in the Task Authorization.

The Contractor's proposed resources must meet the following qualifications:

P1. **Intermediate Project Manager** - Must have a minimum of 4 years' experience within the last 10 years as a Project Manager, including 2 years' experience in managing LMS projects;

P2. **Intermediate Business Analyst** – Must have a minimum of 2 years' experience as a Business Analyst in an IT environment and preferably with LMS applications obtained within the last 5 years.

P3. **Intermediate Information Architect** – Must have a minimum of 2 years' LMS architectural experience obtained within the last 5 years

P4. **Intermediate Change Manager** – Must have a minimum of 4 years' experience obtained within the last 10 years in a change manager role.

P5. **Intermediate Trainer** - Must have delivered a minimum of 60 training days within the last 3 years as a Training Facilitator. If online training facilitation is part of the requirement, then the resource must have delivered a minimum of 60 training hours within the last 3 years as an Online Training Facilitator.

The Contractor must ensure the resources available to provide the professional services support as required and that the assigned resources meet the qualifications identified above as assessed by IRCC. The following table provides an overview of the estimated level of effort in days needed for each of the resource categories identified. IRCC has the right to modify the total number of hours for each category post contract award and as the implementation advances according to the timelines for the various project deliverables.

ESTIMATED LMS PROFESSIONAL SERVICE REQUIREMENTS[1][2]						
	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28	FY 2028-29
LMS Consulting Resources[3]	**Days**	**Days**	**Days**	**Days**	**Days**	**Days**
Intermediate Trainer	130	15	15	10	10	10
Intermediate Project Manager	210	50	50	50	50	50
Intermediate Information Architect	210	20	20	20	20	20
Intermediate Business Analyst	165	50	50	40	40	40
Intermediate Change Manager	165	15	10	10	10	10
TOTALS:	**880**	**150**	**145**	**130**	**130**	**130**

[1] The professional service days indicated are the maximum days allotted per fiscal year. No minimum number of days is required.
[2] The use of Professional services in the contract for all fiscal years are optional
[3] The number of resources utilized to provide the deliverables is up to the Contractor's discretion as long as the total number of days are not exceeded

D 5.3 Delivery Dates

The following table provides estimated delivery dates for some of the key activities related to the set-up configuration, testing, and hand-off the LMS solution to IRCC. Specific timelines will be developed and agreed upon by IRCC and the Contractor following award of contract.

Deliverable	Description	Estimated Delivery Date
Kick Off Meeting	Comprehensive Project Plan; Communication Plan;	1 week following contract award
Planning and Design	Technical Infrastructure Design and Implementation Plan; Training Plan; Requirements Validation Document; System Design Blueprint	6 weeks following kick off meeting
Data and Content integration	Testing Plan(s); Risk Management/ Mitigation plan	10 weeks following contract award
Quality Assurance, Testing and Training	Quality Assurance and Testing Reports; Submission of Complete User System Manual	12 weeks following contract award
Implementation & Support	Support Plan	12 weeks from contract award
Hand-off	IRCC Autonomy	14 weeks from contract award
Acceptance and Close-out & ongoing support	Project Closeout Plan; Implementation Plan; Change Management Plan;	20 weeks from contract award

D6. Limitations and Constraints

The Contractor must meet the security requirements outlined in the *Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103)* https://cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103#annbwhich is a comprehensive set of guidelines and controls based on ITSG-33. The Contractor's Solution must meet the *Government of Canada Security Control Profile for Cloud-Based GC Services* by providing one of the following:

- A valid SOC-2 or SOC-3 report (ISAE-3402);
- ISO-27001 Certification;
- Compliance with U.S. National Institute of Standards and Technology (NIST) Publication 800-53;

D7. Official Languages

The Solution must be available and fully functional in both of Canada's official languages (English and French). All required documentation and support must also be available and provided upon request in both of Canada's official languages (English and French).

D8. Travel

Location of work is at the Contractor's facility. No travel is anticipated. If the Contractor or its resources should travel in person to IRCC facilities, all expenses will be the sole responsibility of the Contractor.

D9. Availability of Personnel

The Contractor certifies that they, its employees and subcontractors will be available to commence performance of the work from the Contract award date and will remain available to perform the work in relation to the fulfillment of this requirement.

D10. Diversity

IRCC is committed to making our Department more inclusive for everyone and fostering an equitable workplace culture that values diversity and creates an environment that is welcoming and rewarding for all. We encourage the businesses that work with us to reflect these values. More information can be found at: https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service2.html

ANNEX A to APPENDIX D – Statement of IRCC LMS Requirements

(See attachment)

APPENDIX E, BASIS OF PAYMENT

During the period of the contract, the Contractor will be paid as specified below, for Work performed in accordance with the Contract.

All deliverables are F.O.B. Destination, and Canadian Customs Duty included and applicable taxes are extra.

For bid evaluation and contractor(s) selection purposes only, the evaluated price of a bid will be determined in accordance with this Basis of Payment, Appendix E.

Canada's total liability to the Contractor under the Contract shall not exceed $_____ *(to be determined at contract award)*, including all options, travel expenses and all applicable taxes.

The Bidder must complete this pricing schedule and include it in its financial bid. Other than completing the required section(s) in the pricing table below, the bidder must not make any other changes or alternations. By doing so will render the bidder's response non-compliant and will be eliminated from the competition.

1. The Bidder should complete this pricing schedule and include it in its financial bid. As a minimum, the Bidder must respond to this pricing schedule by inserting in its financial bid for each of the periods specified below its quoted firm all-inclusive daily rate (in Cdn $) for each of the Consultant Categories identified.
2. The prices or rates specified below, when quoted by the Bidder, include any of the following expenses that may need to be incurred to satisfy the terms of any contract that may result from its bid:
   - **a)** all travel and living expenses for work performed within the National Capital Region (NCR). The NCR is defined in the National Capital Act, R.S.C. 1985, c. N-4, S.2. The National Capital Act is available on the Justice Website;
   - **b)** any travel expenses for travel between the Contractor's place of business and the NCR; and
   - **c)** any travel and living expenses for the relocation of resources to satisfy the terms of any resulting contract. These expenses cannot be charged directly and separately from the professional fees to any contract that may result from the bid solicitation**.**
3. The volumetric data included in the pricing schedule detailed below is provided for bid evaluated price determination purposes only. They are not to be considered as a contract guarantee.

PRICING SCHEDULE

The Contractor will be paid the following all-inclusive **firm unit rates** for the Work pursuant to this Contract. The rates must be all inclusive of any expenditures required to fulfill the Contract. All applicable taxes are extra.

For the One-Time Environment set-up fee, the all-inclusive lot cost includes implementation including set up, assistance with integration and installation of the Solution up to and including the successful completion of the system acceptance as per the approved implementation plan. It also includes the provision of any associated user documentation

For the Subscription Services, the all-inclusive firm unit price includes the provision of Software Documentation, Warranty, Hosting and Maintenance and Support related to the Learning Management System and described in Annex A to Appendix D - Statement of requirements, the Contractor will be paid the firm all-inclusive rates indicated in the Tables 1 and 3, payable annually in advance.

TABLE 1 - LIST OF INITIAL DELIVERABLES

Table 1 - List of Initial Deliverables											
Initial Period: Contract Award to February 28 2026											
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Item No.	**Requirement**	**Part No.**	**SaaS Product Name**	**SaaS Publisher Name**	**Cloud Service Provider Name**	**Unit of Measure**	**Language (EN/FR)**	**Estimated Quantity**	**No. of Years**	**Firm all-inclusive Unit Price (CAD$)**	**Extended Price I x J x K**
YEAR 1: Contract award to February 29 2024											
T1.1	One-time Environment Set up							1	N/A	$	$
T1.2	Subscription Services					Per user		15,000	1	$	$
T1.3										**Sub-Total for Initial Period: YEAR 1**	$
YEAR 2: March 1 2024 to February 28 2025											
T1.4	Subscription Services					Per user		15,000	1	$	$
T1.5										**Sub-Total for Initial Period: YEAR 2**	$
YEAR 3 : March 1 2025 to February 28 2026											
T1.6	Subscription Services					Per user		15,000	1	$	$
T1.7										**Sub-Total for Initial Period: YEAR 3**	$
T1.8										**Sub-Total (Year 1 + Year 2 + Year 3):**	$

TABLE 2 – List of Professional Services “as and when requested” during the initial contract period

For optional professional services requested by Canada, in accordance with an approved Task Authorization (TA), Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked in accordance with the firm all-inclusive per diem rates set out in Tables 2 and 4, applicable taxes extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.

For the Training offerings, the all-inclusive firm unit cost includes the provision of all training material.

Table 2 - List of Professional Services "As and When Requested"				
Initial Period: Contract Award to February 28 2026				
A	**B**	**C**	**D**	**E**
Item No.	**Product Name**	**Estimated level of effort**	**All-inclusive Firm Per Diem or Unit Rate (CAD$)**	**Extended Price for Evaluation Purposes E = C x D**
YEAR 1: Contract award to February 29, 2024				
T2.1	Intermediate Trainer	130 days	$	$
T2.2	Intermediate Project Manager	210 days	$	$
T2.3	Intermediate Information Architect	210 days	$	$
T2.4	Intermediate Business Analyst	165 days	$	$
T2.5	Intermediate Change Manager	165 days	$	$
T2.6	Training Offerings Virtual	1 session	$	$
T2.7	Training Offering In-person/classroom	1 session	$	$
T2.8	**Sub-Total for Initial Period: YEAR 1**			$
YEAR 2: March 1, 2024 to February 28 2025				
T2.9	Intermediate Trainer	15 days	$	$
T2.10	Intermediate Project Manager	50 days	$	$
T2.11	Intermediate Information Architect	20 days	$	$
T2.12	Intermediate Business Analyst	50 days	$	$
T2.13	Intermediate Change Manager	15 days	$	$
T2.14	Training Offerings Virtual	1 session	$	$
T2.15	Training Offering In-person/classroom	1 session	$	$
T2.16	**Sub-Total for Initial Period: YEAR 2**			$
YEAR 3: March 1 2025 to February 28 2026				
T2.17	Intermediate Trainer	15 days	$	$
T2.18	Intermediate Project Manager	50 days	$	$
T2.19	Intermediate Information Architect	20 days	$	$
T2.20	Intermediate Business Analyst	50 days	$	$
T2.21	Intermediate Change Manager	10 days	$	$
T2.22	Training Offerings Virtual	1 session	$	$
T2.23	Training Offering In-person/classroom	1 session	$	$
T2.24	**Sub-Total for Initial Period: YEAR 3**			$
T2.25	**Sub-Total (Year 1 + Year 2 + Year 3)**:			$

Definition of a Day/Proration:

For the purposes of this Contract, a day is defined as 7.5 hours of work, exclusive of meal breaks. Payment will be for days actually worked with no provision for annual leave, statutory holidays and sick leave. If time worked is more or less than a day, the fixed daily rate will be prorated to reflect actual time worked in accordance with the following formula:

Hours worked X applicable firm per diem rate
7.5 hours

1. All proposed personnel must be available to work outside normal office hours during the duration of the Contract.

2. No overtime will be authorized under the Contract. All time worked will be compensated according to the paragraph above.

TABLE 3 – LIST OF DELIVERABLES – OPTION YEARS

Table 3 - List of Deliverables – Option Years											
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Item No.	**Requirement**	**Part No.**	**SaaS Product Name**	**SaaS Publisher Name**	**Cloud Service Provider Name**	**Unit of Measure**	**Language (EN/FR)**	**Estimated Quantity**	No. of Years	**Firm all-inclusive Unit Price (CAD$)**	**Extended Price L = I x J x K**
OPTION YEAR 1: March 1 2026 to February 28 2027											
T3.1	Subscription Services					Per user		15,000	1	$	$
T3.2	**Sub-Total for OPTION YEAR 1**										$
OPTION YEAR 2: March 1 2027 to February 29 2028											
T3.3	Subscription Services					Per user		15,000	1	$	$
T3.4	**Sub-Total for OPTION YEAR 2**										$
OPTION YEAR 3: March 1 2028 to February 28 2029											
T3.5	Subscription Services					Per user		15,000	1	$	$
T3.6	**Sub-Total for OPTION YEAR 3**										$
T3.7	**Sub-Total (Option Year 1 + Option Year 2 + Option Year 3):**										$

TABLE 4 – LIST OF PROFESSIONAL SEVICES 'AS AND WHEN REQUESTED' – OPTION YEARS

Table 4 - List of Professional Services "As and When Requested" – Option Years				
A	**B**	**C**	**D**	**E**
Item No.	**Product Name**	**Estimated level of effort**	**All-inclusive Firm Per Diem or Unit Rate (CAD$)**	**Extended Price for Evaluation Purposes E = C x D**
OPTION YEAR 1: March 1, 2026 to February 28 2027				
T4.1	Intermediate Trainer	10 days	$	$
T4.2	Intermediate Project Manager	50 days	$	$
T4.3	Intermediate Information Architect	20 days	$	$
T4.4	Intermediate Business Analyst	40 days	$	$
T4.5	Intermediate Change Manager	10 days	$	$
T4.6	Training Offerings Virtual	1 sessions	$	$
T4.7	Training Offering In-person/classroom	1 session	$	$
T4.8	**Sub-Total for OPTION YEAR 1:**			$

OPTION YEAR 2: March 1, 2027 to February 29, 2028				
T4.9	Intermediate Trainer	10 days	$	$
T4.10	Intermediate Project Manager	50 days	$	$
T4.11	Intermediate Information Architect	20 days	$	$
T4.12	Intermediate Business Analyst	40 days	$	$
T4.13	Intermediate Change Manager	10 days	$	$
T4.14	Training Offerings Virtual	1 sessions	$	$
T4.15	Training Offering In-person/classroom	1 session	$	$
T4.16	**Sub-Total for OPTION YEAR 2:**			$
OPTION YEAR 3: March 1, 2028 to February 28, 2029				
T4.17	Intermediate Trainer	15 days	$	$
T4.18	Intermediate Project Manager	50 days	$	$
T4.19	Intermediate Information Architect	20 days	$	$
T4.20	Intermediate Business Analyst	40 days	$	$
T4.21	Intermediate Change Manager	10 days	$	$
T4.22	Training Offerings Virtual	1 sessions	$	$
T4.23	Training Offering In-person/classroom	1 session	$	$
T4.24	**Sub-Total for OPTION YEAR 3**			$
T4.25	**Sub-Total (Option Year 1 + Option Year 2 + Option Year 3):**			$

TABLE 5 - LIST OF OPTIONAL ADDITIONAL USERS ACCESS

The Optional Additional Users Access table will not be included in the financial evaluation, however, should any items be exercised during the initial period or option years, the pricing will not exceed an increase of 3% per year. Bidders must complete columns E and F of Table 5.

Table 5 - List of Optional additional users access					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Item No.	**Description**	**Estimated No. of Users**	**Number of months**	**Firm User Price (CAD $)**	**Extended Price F = C x D x E**
T5.1	Additional users access for initial contract period – Year 1	1,000	12	$	$
T5.2	Additional users access for initial contract period – Year 2	1,000	12	$	$
T5.3	Additional users access for initial contract period – Year 3	1,000	12	$	$
T5.4	**Subtotal for the Initial Period (T5.1 + T5.2 + T5.3)**				$
T5.5	Additional users access for option year 1	1,000	12	$	$
T5.6	Additional users access for option year 2	1,000	12	$	$
T5.7	Additional users access for option year 3	1,000	12	$	$
T5.8	**Subtotal for the option years (T5.5 + T5.6 + T5.7)**				$
T5.9	**Sub-Total for Table 5**				$

TABLE 6: TOTAL EVALUATED PRICE FOR CALCULATION

TABLE 6: Total Evaluated Price for Calculation			
(A)	**(B)**	**(C)**	**(D)**
Item No.	**Description**	**Price Calculations**	**Extended Price**
T1	Initial Deliverables		$
T2	Professional Services		$
T3	Deliverables – Option Years		$
T4	Professional Services – Option Years		$
Total Evaluated Price for Evaluation Purposes (T1 + T2 + T3 + T4):			$

APPENDIX F - SECURITY REQUIREMENTS CHECKLIST (SRCL)

Clear Data - Effacer les données

Government of Canada | Gouvernement du Canada

English Instructions | Instructions français

Contract Number / Numéro du contrat
152202-B
Security Classification / Classification de sécurité
Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Immigration Refugee and Citizenship Canada	Learning Academy / HRSB

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

Cloud Based Software as a Solution (SaaS) Learning Management System

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 commerciales 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

Contract Number / Numéro du contrat
152202-B
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? — Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — ☑ No / Non ☐ Yes / Oui
   If Yes, indicate the level of sensitivity: / Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets: — Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? — ☑ No / Non ☐ Yes / Oui
   Short Title(s) of material / Titre(s) abrégé(s) du matériel :
   Document Number / Numéro du document :

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

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

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

Special comments: / Commentaires spéciaux : _____

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — 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? — ☐ No / Non ☑ Yes / Oui

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

Contract Number / Numéro du contrat
152202-B
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	 B	 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 PROTÉGÉ 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.

12. b) Will the document 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).

ANNEX A to APPENDIX F

Contract Security Program – Security Requirement for Canadian Suppliers

PWGSC FILE # 152202-B

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) and obtain approved Document Safeguarding Capability at the level of PROTECTED A, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

3. The Contractor/Offeror MUST NOT utilize its facilities to process, produce, or store PROTECTED information or assets until the CSP, PWGSC has issued written approval.

4. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED A.

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

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

   (a) Security Requirements Check List and security guide (if applicable), attached at Appendix F;
   (b) Contract Security Manual (Latest Edition);
   (c) CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src

NOTE: Any **Contractor or, sub-contractor, or third party delivering Cloud** services must be approved by Canada, and comply with the security requirements in the GC Security Control Profile for Cloud-Based GC IT Services for Protected A, Low Integrity and Low Availability (PALL) for the scope of the proposed Commercially Available Software as a Service (SaaS) provided. Be advised that the Contract Security Program does not assess or approve Cloud solutions in support of any contract. Prior to contract award, **the contractor must** provide evidence, and confirmation to Canada of a Cloud Solution assessment by Canada using the Canadian Centre for Cyber Security (CCCS) - IT Assessment & Supply Chain Integrity (SCI) Assessment (ITSM.50.100) methodologies (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

Furthermore, **the client department IT Security Authority** must perform a local IT assessment against the required controls, and cloud security profiles as determined by CCCS. Suppliers must provide the required information to the IT Security Authority upon request. For more information, guidance, and training on how to conduct this local IT assessment contact CCCS at contact@cyber.gc.ca.

Industrial Security Program – Security Requirements for Foreign Suppliers

PWGSC FILE #: 152202-B, REQUEST FOR PROPOSAL (RFP), RELIABILITY, ACCESS TO AND SAFEGUARDING OF CANADA PROTECTED A INFORMATION, USE OF IT

The Canadian Designated Security Authority (Canadian DSA) is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD). The Canadian DSA is the authority for confirming Contractor compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient Contractor incorporated or authorized to do business in a jurisdiction other than Canada and delivering outside of Canada the services listed and described in the subsequent contract.

1. The Foreign recipient Contractor must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.
2. The Foreign recipient Contractor must, at all times during the performance of the contract, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:
    i. The Foreign recipient Contractor must provide proof that they are incorporated or authorized to do business in their jurisdiction.
    ii. The Foreign recipient Contractor must not begin the work, services or performance until the Canadian DSA is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient Contractor in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.
    iii. The Foreign recipient Contractor must identify an authorized Contract Security Officer (CSO) and an Alternate (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in the contract. This individual will be appointed by the proponent foreign recipient Contractor's Chief Executive Officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.
    iv. The Foreign recipient Contractor must not grant access to CANADA PROTECTED A information/assets, except to its personnel subject to the following conditions:
        a. Personnel have a need-to-know for the performance of the contract;
        b. Personnel have been subject to a Criminal Record Check, with favourable results, from a recognized governmental agency or private sector organization in **their country** as well as a Background Verification, validated by the Canadian DSA.
        c. The Foreign recipient **Contractor** must ensure that personnel provide consent to share results of the Criminal Record Check(s) with the Canadian DSA and other Canadian Government Officials, if requested; and
        d. The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor** for cause.
3. **CANADA PROTECTED** information/assets provided or generated pursuant to this **contract** must not be further provided to a third party Foreign recipient Subcontractor unless:
    i. written assurance is obtained from the Canadian DSA to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **CANADA PROTECTED** information/assets by the Canadian DSA; and
    ii. written consent is obtained from the Canadian DSA, if the third-party Foreign recipient Subcontractor is located in a third country.

4. The Foreign recipient **Contractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor** must ensure that its personnel are made aware of and comply with this restriction.
5. The Foreign recipient **Contractor** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.
6. The Foreign recipient **Contractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC at the level of **CANADA PROTECTED A.**

All **CANADA PROTECTED** information/assets, furnished to the foreign recipient **Contractor** or produced by the foreign recipient **Contractor**, must also be safeguarded as follows:

7. The Foreign recipient **Contractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets pursuant to this **contract** has been compromised.
8. The Foreign recipient **Contractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets accessed by the foreign recipient **Contractor**, pursuant to this **contract**, have been lost or disclosed to unauthorized persons.
9. The Foreign recipient **Contractor** must not disclose **CANADA PROTECTED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.
10. The Foreign recipient **Contractor** must provide the **CANADA PROTECTED** 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 Canadian DSA.
11. Upon completion of the Work, the foreign recipient **Contractor** must return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **contract**, including all **CANADA PROTECTED** information/assets released to and/or produced by its subcontractors.
12. The foreign recipient **Contractor** requiring access to **CANADA PROTECTED A** information/ assets, under this **contract**, must submit a Request for Site Access to the Chief Security Officer of **Citizenship and Immigration Canada**.
13. The Foreign recipient **Contractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any **CANADA PROTECTED A** information/assets until authorization to do so has been confirmed by the Canadian DSA.
14. In the event that a foreign recipient **Contractor** is chosen as a supplier for this **contract**, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.
15. 15. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of the Canadian DSA.
16. All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
17. All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
18. The Foreign recipient **Contractor** must comply with the provisions of the Security Requirements Check List attached at Appendix F.

19. Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

APPENDIX G – Security and Privacy Obligations

Schedule 1 - Security Obligations

Purpose

The purpose of this Schedule is to set forth the obligations of the Contractor relating to the proper management of Canada's Data, including protection from unauthorized modification, access or exfiltration, in accordance with the contract, this Schedule, and the Contractor's Security Measures (collectively, the "**Security Obligations**").

Flow-Down of Security Obligations

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Sub-processors and/or Subcontractors to the extent applicable.

Change Management

The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Requirements as needed to comply with the security best practices and industry standards as set forth in this Schedule.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse affect to the Cloud Services offerings in this Contract, including technological, administrative or other types of changes or improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

20. Acknowledgements

The parties acknowledge that:

(a) Canada's Data is subject to these Security Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Canada's Data.

(c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(d) Security Obligations apply to Tier 2 (up to and including Protected B / Medium Integrity, Medium Availability or Medium Injury), unless otherwise specified.

21. Securing Canada's Data

(1) The Contractor must protect Canada's Data from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate technical and organizational security measures including information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Canada's Data.

22. Roles and Responsibilities for Security

a. The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the Cloud Services between the Contractor and Canada. This includes, at a minimum, the roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.

b. The Contractor must provide to Canada an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there are significant changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of Canada.

23. Third-Party Assurance: Certifications and Reports

a. The Contractor must ensure that Canada's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured with appropriate security measures that comply with the requirements set forth in the Contractor's security practices and policies.

b. The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications and audit reports by providing independent third party assessment reports or certifications that addresses each service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering, including:

   i. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; AND

   ii. ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body; AND

   iii. AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality - issued by an independent Certified Public Accountant.

c. Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If there are any exclusions identified, or there is a need to separate a subservice organizations such as data centre hosting, the subservice organization's assessment report must be provided.

d. Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

e. Each SOC 2 Type II audit report must have been performed within the 12 months prior to the start of the contract. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

f. The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and SOC 2 Type II for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

24. Auditing Compliance

a. The Contractor must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Canada's Data as follows:

i. Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

ii. Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

iii. Each audit will be performed by independent, third party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

b. Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

c. Upon request of Canada, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

25. Cloud Service Provider (CSP) IT Security Assessment Program

a. Within the initial contract period, the Contractor must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM)
(https://cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103#annb) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

b. Compliance will be assessed and validated by IRCC in accordance with CCCS guidelines for localized IT security assessments. https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100

The Contractor must demonstrate that they participated in the process by successfully on-boarded, participated in, and completed the program. This includes providing the following documentation:

i. A copy of the confirmation letter that confirms that they have on-boarded into the program;
ii. A copy of the most recent completed assessment report provided by CCCS; and
iii. A copy of the most recent summary report provided by CCCS.

The Contractor should contact the CCCS Client Services, as indicated in Appendix L, SaaS IT Security Assessment Program, for any additional information related to the CSP IT Assessment Program.

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify CCCS when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

Certifications identified below, and validated through independent third party assessments.

b In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 4 - Third-Party Assurance and Section 6 - Cloud Service Provider (CSP) IT Security Assessment Program, sub-sections (1) and (2) the SaaS provider must provide Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Contractor has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a final report with regards to the assessment. For any questions, CCCS can be contacted by email at contact@cyber.gc.ca.

26. Data Protection

a The Contractor must:

i. Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 13 - Cryptographic Protection.

ii. Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with Section 13 - Cryptographic Protection and Section 21- Network and Communications Security.

iii. Implement security controls that restricts administrative access to Canada's Data and Systems by the Contractor and provides the ability to require the approval of Canada before the Contractor can access Canada's Data to perform support, maintenance or operational activities.

iv. Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to Canada's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or customer support, based on approval from Canada.

b The Contractor must not make any copies of databases or any part of those databases containing Canada's Data outside of regular service resilience capabilities and within approved regional spaces or zones within Canada.

c The Contractor must ensure that any processing performed outside of Canada including moving or transmitting approved copies of data are performed within the agreed upon service regions.

d Upon request of Canada, the Contractor must provide Canada with a document that describes all additional metadata created from Canada's Data.

27. Data Isolation

a. The Contractor must implement controls to ensure appropriate isolation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Cloud Services and Contractor Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

i. The separation between Contractor's internal administration from resources used by its customers;
ii. The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and
iii. Ability for the GC to support isolation within GC-managed tenant environment.

b. Upon request of Canada, the Contractor must provide Canada with a document that describes the approach for ensuring appropriate isolation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit.

28. Data Location

a. The Contractor must store and protect Canada's Data, at rest, including data in backups or maintained for redundancy purposes. This includes the ability to isolate data in Canada in approved data centers. An approved Data Centre is defined as the following:

i. A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security;
ii. Ensures the infeasibility of finding a specific customer's data on physical media; and
iii. Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 13 - Cryptographic Protection.

b. The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

c. The Contractor must have the ability for Canada to isolate Canada's Data hosted in Cloud Services in data centers that are geographically located in Canada.

d. Upon request of Canada, the Contractor must:

i. Provide the GC with an up-to-date list of the physical locations, including city, which may store Canada's Data at rest; and

ii. Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

e. It is the continuous obligation of the Contractor of the proposed Cloud Services to notify Canada when there are updates to the list of physical locations which may store Canada's Data at rest.

29. Data Transfer and Retrieval

The Contractor must provide the capability including tools and services that allow Canada to:

a. Extract all online, nearline, and offline Canada's Data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

b. Securely transfer all Canada's Data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/governmentinformation-resources/guidelines/Pages/guidelines-file-formats-transferring-informationresources-enduring-value.aspx).

30. Data Disposition and Returning Records to Canada

a. The Contractor must securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Canada's Data and ensure that previously stored data cannot be addressed by others customers after it is released. This includes all copies of Canada's Data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following:

   i. National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

b. The Contractor must provide Canada with confirmation that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once Canada discontinues its use of the Cloud Services.

31. Cryptographic Protection

The Contractor must:

a. Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods;

b. Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111);

c. Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/groupgroupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree

of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and

d. Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.

32. Key Management

The Contractor must ensure that a key management service can be leveraged and provides capabilities, including but not limited to:

a. Creation/generation and deletion of encryption keys by the GC;

b. Definition and application of specific policies that control how keys can be used;

c. Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;

d. Ability to audit all events related to key management services, including Contractor access for Canada's review;

e. Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;

f. Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and

g. Ability to delegate key use privileges for use by the Cloud Services used for the GC-managed services.

33. Endpoint Protection

The Contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.

34. Secure Development

The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

35. Identity and Access Management

a. The Contractor must have the ability for Canada to support secure access to Cloud Services including ability to configure:

i. multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;
ii. Role-based access;
iii. Access controls on objects in storage; and
iv. Granular authorization policies to allow or limit access.

b. The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

36. Federation

The Contractor must have the ability for Canada to support federated identity integration including:

a. Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0, or subsequent versions, where the End User credentials and authentication to cloud services are under the sole control of Canada; and

b. Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding Cloud Service user account(s).

37. Privileged Access Management

(1) The Contractor must:

a. Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;

b. Restrict and minimize access to the Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;

c. Enforce and audit authorizations for access to the Cloud Services and Canada's Data;

d. Constrain all access to service interfaces that host Canada's Data to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);

e. Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

f. Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

g. Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

h. Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Canada's Data;

i. Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

j. Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and Canada's Data;

k. Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Cloud Services and Contractor Infrastructure;

l. Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and

m. Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring privileged access of the Cloud Services.

38. Remote Management

a. The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that are used to host GC services and take reasonable measures to:

i. Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

ii. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 13 (Cryptographic Protection);

iii. Route all remote access through controlled, monitored, and audited access control points;

iv. Expeditiously disconnect or disable unauthorized remote management or remote access connections;

v. Authorize remote execution of privileged commands and remote access to security-relevant information.

b. Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Services.

39. Network and Communications Security

The Contractor must:

a. Enforce secure connections to the Cloud Services, including providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;

b. Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);

c. Use correctly configured certificates within the TLS connections in accordance with CSE guidance.

d. Provide the ability for Canada to implement network access controls and security rules that allow or deny network traffic to Canada resources.

40. Logging and Auditing

a. The Contractor must implement log generation and management practices and controls for all Cloud Service components that store or process Canada's Data, and that conform with industry standards and best practices, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented log generation and management practices and controls.

b. The Contractor must provide the ability for Canada to export security event logs using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.), for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

c. The Contractor must enable Canada to centrally review and analyze audit records from multiple components from the Cloud Services consumed by the customer. This includes providing APIs that provide the ability to inspect and interrogate data at rest in SaaS applications including assessing events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access stored in SaaS application logs.

41. Continuous Monitoring

a. The Contractor must continually manage, monitor, and maintain the security posture of Contractor Infrastructure and Service Locations hosting Canada's Data throughout the contract, and ensure that the Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

i. Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or Canada's Data;

ii. Undertake best efforts to prevent attacks through security measures such as denial of service protections;

iii. Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

iv. Identify unauthorized use and access of any Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Cloud Service;

v. Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

vi. Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and

vii. Where required, take proactive countermeasures, including taking both preemptive and responsive actions, to mitigate threats.

b. The Contractor's Cloud Services must allow for GC application data of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

42. Security Incident Management

(a) The Contractor Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

i. A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

ii. Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the information security incidents that the Contractor will report to Canada; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents; and (vi) any remedies that apply if certain information security occur.

iii. Ability for the Contractor to support Canada's investigative efforts for any compromise of the users or data in the service that is identified.

iv. Allows only designated representatives of Customer (e.g. SSC Security Operations Center) authorized by the Technical Authority:

a. to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
b. the ability for Customer to track the status of a reported information security event.

v. Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and includes forensic procedures and safeguards for the maintenance of a chain of custody;

(b) Upon request of Canada, the Contractor must provide a document that describes the Contractor's Security Incident Response Process.

The Contractor must:

a. Work with Canada's Security Operations Center(s) (e.g. CCCS, Departmental SOC) on Security Incident containment, eradication and recovery in accordance with the Security Incident Response process.

b. Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and

c. Track, or enable Canada to track, disclosure of Canada's Data, including what data has been disclosed, to whom, and at what time.

(c) Canada may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor agrees to provide assistance to the GC on a best effort basis.

43. Security Incident Response

a. The Contractor must alert and promptly notify Canada (via phone and/or email) of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security malfunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 72 hours, and within the Contractor's service level commitments.

b. If the Contractor becomes aware of any compromise, breach and determines a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

44. Information Spillage

a. The Contractor must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Contractor's Information Spillage process must include, at a minimum:

i. A process for identifying the specific data elements that is involved in a System's contamination;

ii. A process to isolate and eradicate a contaminated System; and

iii. A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

b. Upon request of Canada, the Contractor must provide a document that describes the Contractor's Information Spillage Response Process.

45. Security Testing and Validation

a. The Contractor must have a process that allows Canada to conduct a non-disruptive and non-destructive Vulnerability Scan or Penetration Test of Canada's portion of the Cloud Service components within the Contractor environment.

The Contractor must provide the ability to enable a self-service security health check or scoring tool that enables the measurement of the security posture of the Cloud Services configured by Canada.

46. Personnel Security Screening

a. The Contractor must ensure that security measures are implemented to grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed.

b. The Contractor screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

c. Upon request of Canada, the Contractor must provide a document that describes the Contractor's personnel security screening process. The process must provide, at a minimum:

i. A description of the employee and Sub-processor positions that require access to Customer Data or have the ability to affect the confidentiality, integrity or availability of the Cloud Services;

ii. A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

iii. A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;

iv. A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;

v. The approach to detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of Cloud Services hosting Canada's data.

47. Physical (Data Centre / Facilities) Security

a. The Contractor must ensure that physical security measures are implemented to protect the IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control

(https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611). The security measures required under this include, at a minimum:

i. Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and Canada's Data within the prescribed service level commitments;

ii. Proper handling of IT Media;

iii. Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;

iv. Controlled access to information system output devices to prevent unauthorized access to Canada's Data;

v. Limiting physical access to Canada's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

vi. Escorting visitors and monitoring visitor activity;

vii. Enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and

viii. Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting Canada's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.

b. Upon request of Canada, the Contractor must provide a document that describes the Contractor's physical security measures.

c. If any physical security measures is to change in a way that materially degrades the physical security, the Contractor must inform Canada.

48. Supply Chain Risk Management

a. The Contractor must ensure that safeguards are implemented to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain.

b. The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management Plan that is aligned with one of the following best practices:

i. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);

ii. NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or

iii. ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

c. Within 90 days of contract award, the Contractor must:

i. Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime

OR

ii. Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

d. In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

49. Sub-processors

a. The Contractor must provide a list of Sub-processors that could be used to perform any part of the Work in providing Canada with the Service. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Work that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Work.

b. The Contractor must provide a list of Sub-processors within ten days of the effective date of the Contract. The Supplier must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Customer Data or Personal Data. The Supplier must assist Canada with verification of sub-processors within 10 working days.

Schedule 2 – Privacy Obligations

General

Purpose

The purpose of this Schedule is to set forth the privacy obligations of the Contractor relating to the use, collection, processing, transmission, storage or disposal of Canada's Data containing Personal Information (PI). Any Personal Information which is stored on Contractor systems or the Contractor is required to handle (collect, retain, use, disclose and dispose) must be safeguard at all times by implementing administrative, physical and technical safeguards that are necessary to ensure the PI is protected commensurate to the level of injury that could arise if a privacy breach was to occur and in accordance with the Contractor Data Processing Agreement, this Schedule, and the Contractor's Specific Privacy Measures (collectively, the "**Privacy Obligations**").

Flow-Down of Privacy Obligations

The obligations of the Contractor contained in these Privacy Obligations must be flowed down by the Contractor to Sub-processors and/or Subcontractors, to the extent applicable.

Change Management

The Contractor must, throughout the Contract, take all steps required to update and maintain the Privacy Obligations as needed to comply with the security practices of industry standards.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse affect to the Cloud Service offerings in this Contract, including technological, administrative, or other types of changes or improvements that are made, and that could impact the current collection, use, disclosure and or disposal of data containing personal information. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

1. **Acknowledgments**

The parties acknowledge that:

(a) All Canada's Data containing personal information are subject to these Privacy Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and privacy controls relating to Canada's Data.

(c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Contractor Personnel to access Canada's Data prior to the implementation of the Privacy Obligations as required under this Schedule on or before the date of Contract Award.

2. **Data Ownership**

(1) Canada will at all time remain the controller of the Personal Information (PI) processed by the Contractor under the Contract. Canada is responsible for compliance with Canada's privacy obligations as a controller under applicable data protection law, in particular for justification of any transmission of PI to the Contractor (including providing any required notices and obtaining any required consents and/or authorizations, or

otherwise securing an appropriate legal basis under applicable data protection law), and for Canada's decisions and actions concerning the processing of such personal data.

(2) The Contractor is and will at all times remain a processor with regard to the data containing PI provided by Canada to the Contractor under the Contract. The Contractor is responsible for compliance with its obligations under this it's Contractor Data Processing Agreement and for compliance with its obligations as a processor under applicable privacy law (i.e. Personal Information Protection and Electronic Documents Act (PIPEDA).

(3) The Contractor must not use or otherwise process Canada's Data containing PI or derive information from it for any data sharing, advertising or similar commercial purposes. As between the parties, Canada retains all right, title and interest in and to Customer Data. The Contractor acquires no rights in Customer Data, other than the rights Customer grants to the Contractor to provide the Cloud Services to Customer.

(4) All data that is stored, hosted or processed on behalf of Canada remains the property of Canada.

3. Privacy Requests

(1) Canada and the Contractor must establish a mutually agreeable process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).

(2) Within 30 calendar days of Contract award, the Contractor must provide a document that describes how the Contractor will support Canada in handling Access Requests, including how it will acknowledge the receipt of an Access Request, and how it will provide the requested information.

4. Third-Party Assurance: Certifications

(1) The Contractor must ensure that in respect of any personal information including Canada's Data that it may host, store or process, on Contractor Infrastructure (including any Iaas, PaaS or SaaS Service provided to Canada) and Service Locations are secured appropriate privacy and security measures that comply with the requirements set forth the Contractor's privacy practices and policies.

(2) The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications by providing independent third party assessment reports or certifications that addresses each service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering, including:

a. ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Certification achieved by an accredited certification body.

(3) Each certification provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4) Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

(5) The Contractor is expected to maintain its certification of ISO 27018 for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

5. Privacy Compliance

(1) The Contractor must demonstrate through third party assessment reports and audit reports that it:

(a) Restricts creating, collecting, receiving, managing, accessing, using, retaining, sending, disclosing and disposing of Personal Information to only that which is necessary to perform the Cloud Services and;

(b) Has implemented updated security processes and controls such as access management controls, human resource security, cryptography and physical, operational and communications security that preserve the integrity, confidentiality and accuracy of all information and data and metadata, irrespective of format.

6. Auditing Compliance

(1) In the event Canada needs to conduct security and privacy audits, inspections and/or review any additional information (e.g., documentation, data flows, data protection description, data architecture and security descriptions), both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(2) The Contractor must conduct the privacy and security audits of the computers, computing environment and physical data centers that it uses in processing Canada's Data containing PI as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by qualified, independent, third party security auditors that (i) is qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conforms to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(3) Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(4) Upon request of Canada, additional supplementary evidence from the Contractor, including system security and privacy plans, designs, or architecture documents that provide a comprehensive system description including all the data elements containing PI, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

7. Privacy by Design

The Contractor must demonstrate that it implements privacy by design as part of its software development lifecycle, and in accordance with Schedule 1 – Security Obligations, Section 16 (Secure Development).

8. Privacy Officer

The Contractor must, within 10 days of the effective date of this Contract, provide Canada with information that identifies an individual as a Privacy Officer to act as Contractor's representative for all matters related to the Personal Information and the Records. The Contractor must provide that person's name and contact information including the, individual's business title, email address and phone number.

9. Assist in Delivery of Canada's Privacy Impact Assessment

The Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308), by assisting the Canada with the supporting documentation including a foundational PIA for Canada provided by the Contractor. The Contractor agrees to provide this support within five to ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

10. Privacy Breach

(1) The Contractor must promptly evaluate and respond to incidents that create suspicion of or indicate unauthorized access to or processing of Personal Information ("**Incident**"). To the extent the Contractor becomes aware of and determines that an Incident qualifies as a breach of privacy leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed on the Contractor's systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such Personal Information ("Personal Information Breach"), the Contractor will inform Canada of such Personal Information Breach without undue delay, and in accordance with Schedule 1 – Security Obligations, Section 26

(2) The Contractor must:

(a) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data; and

(b) Tracks, or enables Canada to track, disclosures of Canada's Data, including what data has been disclosed, to whom, and at what time.

11. PERSONAL INFORMATION

The following sub-sections applies to situations where the Contractor confirms that it has access, care, and control of Canada's data.

11.1 Ownership of Personal Information and Records

To perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor/Sub-processor/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

11.2 Use of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Cloud Services in accordance with the **contract**.

Collection of Personal Information

If the foreign recipient **Contractor/Sub-processor/Subcontractor** must collect Personal Information from a third party to perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** must only collect Personal Information that is required to perform the Cloud Services. The foreign recipient **Contractor/Subprocessor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Sub-processor/Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:

(a) that the Personal Information is being collected on behalf of, and will be provided to, Canada;

(b) the ways the Personal Information will be used;

(c) that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;

(d) the consequences, if any, of refusing to provide the information;

(e) that the individual has a right to access and correct his or her own Personal Information; and

(f) that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor/Sub-processor/Subcontractor** .

(2) The foreign recipient **Contractor/Sub-processor/Subcontractor** and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

(3) If requested by the Contracting Authority, the foreign recipient **Contractor/Subprocessor/Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor/Sub-processor/Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

(4) At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Sub-processor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor/Sub-processor/Subcontractor** must ask the Contracting Security Authority for instructions.

11.3 Maintaining the Accuracy, Privacy, and Integrity of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient

Contractor/Sub-processor/Subcontractor must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Subprocessor/Subcontractor** must:

(a) not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

(b) segregate all Records from the foreign recipient **Contractor's/Subprocessor's/Subcontractor's** own information and records;

(c) restrict access to the Personal Information and the Records to people who require access to perform the Cloud Services (for example, by using passwords or biometric access controls);

(d) provide training to anyone to whom the foreign recipient **Contractor/Subprocessor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Cloud Services. The foreign recipient **Contractor/Sub-processor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor/Subprocessor/Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;

(e) if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor/Sub-processor/Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

(f) keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

(g) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor/Sub-processor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Sub-processsor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

(h) keep a record of the date and source of the last update to each Record;

(i) maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor/Sub-processor/Subcontractor** and Canada at any time; and

(j) secure and control access to any hard copy Records.

11.4 Safeguarding Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality, in accordance with the security measures outlined in Schedule 1 – Security Obligations.

11.5 Statutory Obligations

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, *Access to Information Act*, R.S. 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to comply with the requirements established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

(2) The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that its obligations under the **contract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient **Contractor/Sub-processor/Subcontractor** believes that any obligations in the **contract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract** and the specific obligation under the law with which the foreign recipient **Contractor/Subprocessor/Subcontractor** believes it conflicts.

11.6 Legal Requirement to Disclose Personal Information

(1) If the Contractor receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the processing of Personal Information (“Disclosure Request”), it will promptly pass on such Disclosure Request to Canada without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

(2) At Canada’s request, the Contractor will provide Canada with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for Canada to respond to the Disclosure Request in a timely manner.

11.7 Complaints

Canada and the foreign recipient **Contractor/Sub-processor/Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

11.8 Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

APPENDIX H - Supply Chain Integrity Process

Supply Chain Integrity Process

1. **Mandatory Requirements**
   - **1.1. Contractors must submit, with their Submission, the following SCSI:**
     - 1.1.1. **IT Product List:** Contractors must identify the SaaS Solution over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work and/or Services described in the resulting contract. In regards to the SaaS Solution, by completing the Form 3 - SCI Submission Template as provided in the RFP, which includes following information :
       a. **OEM Name:** Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.
       b. **OEM DUNS Number:** Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C – Ownership Information". ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.
       c. **Product Name:** Enter the OEM's name for the product.
       d. **Model Number:** Enter the OEM's model and/or version number of the product.
       e. **Product URL:** Enter the URL of the OEM's webpage for the product.
       f. **Vulnerability Information:** Enter information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers separated by semi-colons (;). If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to IRCC. If this is the case for a particular product, enter "see attached information" in the Vulnerability Information field, and include the filename(s) in the additional information column which provide the required vulnerability information.
     - **1.1.2 Ownership Information:** Contractors must identify the original equipment manufacturer (OEM) of the product(s) or service(s) ordered, as well as the name of any supplier (i.e. subcontractors (individuals or companies), sub-contractors of sub-contractors (individuals or companies) down the chain, re-seller, distributor, sub-processors, etc.) of the product(s) or service(s) that are being ordered. This list must identify all third parties who may perform any part of the Work, whether they would be subcontractors to the Contractor, or subcontractors to subcontractors of the Contractor down the chain. Any subcontractor that could have access to Canada's Data must be identified. For the purposes of this requirement, a third party who is merely a supplier of goods to the Contractor, but who does not perform any portion of the Work, is not considered to be a subcontractor. Subcontractors would include, for example, technicians who might be deployed or maintain the Contractor's solution. If the Contractor does not plan to use any subcontractors to perform any part of the Work, the Contractor is requested to indicate this in its response.

Contractors are requested to provide their information on Form 3. It is requested that Contractors indicate their legal name on each page, insert a page number as well as the total number of pages. Contractors are also requested to insert a separate row for each subcontractor and additional rows as may be necessary.
For each of these entities listed, provide either:

a. **OEM DUNS Number:** Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a

businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.

b. **Country / Nationality:** The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.
c. **Corporate website link:** For each of OEM or Contractor name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.

1.1.3 Network Diagrams: one or more conceptual network diagrams that collectively show the complete network proposed to be used to deliver the services described in the Statement of Work. The network diagrams are only required to include portions of the Contractors' network (and its subcontractor' network(s)) over which Canada's Data, would be transmitted in performing any resulting contract. As a minimum the diagram must show:

i. The following key nodes for the delivery of the services under the resulting contract of this solicitation process, if applicable the role of the Contractor or subcontractor;
    i. Service delivery points;
    ii. Core network;
    iii. Subcontractor network (specifying the name of the subcontractor as listed in the **Ownership Information);**
ii. The node interconnections, if applicable
iii. Any node connections with the Internet; and
iv. For each node, a cross-reference to the product that will be deployed within that node, using the Excel row number from the IT Product List.

1.1.4 List of subcontractors: The tenderer must submit a list of all the subcontractors who could participate in the execution of a part of the work (this includes the subcontractors who are affiliated or linked to it) in the framework of any awarded contract. At a minimum, the list should include the following:

i. the name of the subcontractor;
ii. the address of the subcontractor's head office;
iii. the part of the work that the subcontractor would carry out;
iv. the place or places where the subcontractor would carry out the work.

2. Assessment of Supply Chain Security Information

2.1. Canada will assess whether, in its opinion, the Supply Chain Security Information creates the possibility that the Contractor's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.
2.2. In conducting its assessment:
    a. Canada may request from the Contractor any additional information that Canada requires to conduct a complete security assessment of the Supply Chain Security Information. The Contractor will have 2 working days (or a longer period if specified in writing by the Supply Chain Security Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the response being disqualified.
    b. Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the response or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the Supply Chain Security Information.
2.3. If, in Canada's opinion, any aspect of the Supply Chain Security Information, if used in a

solution, creates the possibility that the Contractor's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

a. Canada will notify the Contractor in writing (sent by email) and identify which aspect(s) of the Supply Chain Security Information is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Contractor regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Contractor; therefore, in some circumstances, the Contractor will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Contractor's Supply Chain Security Information.
b. The notice will provide the Contractor with one opportunity to submit revised Supply Chain Security Information within the 10 calendar days following the day on which Canada's written notification is sent to the Contractor, (or a longer period specified in writing by the Supply Chain Security Authority).
c. If the Contractor submits revised Supply Chain Security Information within the allotted time, Canada will perform a second assessment. If Canada determines that any aspect of the Contractor's revised Supply Chain Security Information could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, no further opportunities to revise the Supply Chain Security Information will be provided and the response will be disqualified.

2.4. By participating in this process, the Contractor acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. Also, the Contractor acknowledges that Canada's security assessment does not involve the assessment of a proposed solution. As a result:

a. qualification pursuant to this RFP does not constitute an approval that the products or other information included as part of the Supply Chain Security Information will meet the requirements of the subsequent bid solicitation or any resulting contract or other instrument that may be awarded as a result of any subsequent bid solicitation;
b. qualification pursuant to this RFP does not mean that the same or similar Supply Chain Security Information will be assessed in the same way for future requirements;
c. at any time during the subsequent bid solicitation process, Canada may advise a Contractor that some aspect(s) of its Supply Chain Security Information has become the subject of security concerns. At that point, Canada will notify the Respondent and provide the Contractor with an opportunity to revise its Supply Chain Security Information, using the same process described above.
d. during the performance of a subsequent contract, if Canada has concerns regarding certain products, designs or subcontractors originally included in the Supply Chain Security Information, the terms and conditions of that contract will govern the process for addressing those concerns.

2.5. All Contractors will be notified in writing regarding whether or not they have qualified under this RFP to proceed to the next stage of the procurement process.

2.6. Any Contractorr that has qualified under this RFP will be required, when responding to any subsequent bid solicitation under this solicitation process, to propose a solution consistent with the final version of the Supply Chain Security Information it submitted with its response to this RFP (subject to revision only pursuant to the paragraph below). Except pursuant to the paragraph below, no alternative or additional Products or subcontractors may be proposed in the Contractor's solution. This is a mandatory requirement of this solicitation process. The proposed solution during any subsequent bid solicitation does not need to contain all the Products within the final Supply Chain Security Information.

2.7. Once a Contractor has been qualified in response to this RFP, no modifications are permitted to the Supply Chain Security Information except under exceptional circumstances, as determined by Canada. Given that not all the exceptional circumstances can be foreseen, whether changes may be made and the process governing those changes will be determined by Canada on a case-by-case basis.

APPENDIX I, TASK AUTHORIZATION FORM

TASK AUTHORIZATION REQUEST			
1.0 Administrative Information:			
Contractor :			
PR Number:	**Contract Number:**		**Date:**
Task Authorization No.:	**PO Number:**		**Response Required by:**
2.0 Description of Work to be performed:			
Background: **General Purpose and Scope:** **Tasks and Responsibilities:** **Deliverables:**			
3.0 Period of services	**From:** **To:**		
4.0 Work location			
5.0 Travel requirements			
6.0 Required Security Clearance	☐ Reliability ☐ Confidential ☐ Secret ☐ Not Applicable		
7.0 Gov't furnished equipment/material			
8.0 Authorities			
IRCC Project Authority:		**IRCC Contracting Authority:**	
9.0 Task Authorization Basis of Payment			
Type of Labour Category	**Fixed All-inclusive Per Diem Labour Rate (CAD $)**	**Estimated Level of Effort (Days)**	**Total Price (CAD $)**
		Subtotal - Labour:	
		Travel Costs:	
		Other Direct Expenses:	
		Subtotal - All:	
		Applicable Taxes:	
		TOTAL:	
Basis of payment			
Limitation of Expenditure			
Method of payment			
Monthly			
Invoice Submission			

TASK AUTHORIZATION APPROVALS	
10.0 IRCC Contracting Authority - Concurrence to Proceed with TA:	
Signature:	**Date:**
11.0 IRCC Project Authority - Contractor's TA Proposal is Accepted:	
Signature:	**Date:**
12.0 Contractor - Concurrence with Expenditure:	
Signature:	**Date:**
You are requested to sell to Canada, in accordance with the terms and conditions included in the IRCC Contract no._____ and the terms and conditions set out herein, referred to herein or attached hereto, the services listed herein for this Task Authorization at the price set out thereof**.**	

APPENDIX J – SaaS Service Level Agreements (SLA)

Only terms and conditions in the SLA, detailed under 3.2 Section I: Technical Bid, article (c) vi, related to service levels and service delivery will be part of the Contract.

By presenting a Bid, the Bidder acknowledges and agrees that any terms contained in Appendix J – SaaS Solution Service Level Agreements that purport to interpret the Contract, are the same or similar subject matter, or are related to the terms contained in the Contract Clauses, are deemed stricken and are of no force or effect. Similarly, any terms contained in Appendix J – SaaS Solution Service Level Agreements which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.

No terms purporting to abridge or extend the time to commence an action for breach, tort, or other action are of any effect.

APPENDIX K, Non-Disclosure Agreement

Note to Contractors: Please note that this Non-Disclosure Agreement only covers Supply Chain Integrity requirements under Article 3.6, Section IV Supply Chain Integrity Requirements.

Non-Disclosure Agreement

By presenting a Submission, the Contractor agrees to the terms of the non-disclosure agreement below (the "**Non- Disclosure Agreement**"):

1. The Contractor agrees to keep confidential any information it receives from Canada regarding Canada's assessment of the Contractor's Supply Chain Security Information (the "**Sensitive Information**") including, but not limited to, which aspect of the Supply Chain Security Information is subject to concern, and the reasons for Canada's concerns.

   Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise and whether or not that information is labeled as classified, proprietary or sensitive.

2. The Contractor agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Contractor who has a security clearance commensurate with the level of Sensitive Information being accessed, without the prior written consent of the Supply Chain Security Authority. The Contractor agrees to immediately notify the Supply Chain Security Authority if any person, other than those permitted by this Article, accesses the Sensitive Information at any time.

3. All Sensitive Information will remain the property of Canada and must be returned to the Supply Chain Security Authority or destroyed, at the option of the Supply Chain Security Authority, if requested by the Supply Chain Security Authority, within 30 days following that request.

4. The Contractor agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Contractor, or immediate termination of any resulting Contract(s). The Contractor also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Contractor's security clearance and review of the Contractor's status as an eligible Contractor for other requirements.
5. This Non-Disclosure Agreement remains in force indefinitely.

APPENDIX L – Tier 1 Security Requirements

Security Requirements for Software as a Service

QUALIFICATION REQUIREMENTS

The following **fifteen (15) Security Requirements** must be met in order to demonstrate compliance with Tier 1 Assurance **(Up to and including Protected A Data).**

1. Tier 1 Assurance (Up to and including Protected A Data)

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M1	**Roles and Responsibilities for Security**	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Solution between the Supplier (any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.
M2	**Data Protection**	a. The physical locations of the Commercially Available Public Software as a Service (which may contain Canada's data) and define in the must be located in either: A country within the North Atlantic Treaty Organization (NATO); b. A country within the European Union (EU); or c. A country with which Canada has an international bilateral industrial security instrument Suppliers please note: Additional information on countries within NATO can be located at the following link: https://www.nato.int/cps/en/natohq/nato_countries.htm Additional information on countries within the EU can be located at the following link: https://europa.eu/european-union/about-eu/countries_en The Contract Security Program has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-rc/international-eng.html and as updated from time to time.	The Supplier must provide documentation that demonstrates how the proposed Commercially Available Public Software as a Service submitted meets the mandatory requirement outlined in Data Protection Requirements. To be considered compliant, the provided documentation must include: a) an up-to-date list of the physical locations (including city and country) for each data centre that may contain Canada's data including in backups or for redundancy purposes. The substantiation required for Data Protection Requirements. The documentations cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M3	**Data Center Facilities**	The Supplier of the proposed Commercially Available Public Software as a Service must implement security measures that ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. This includes, at a minimum a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; d) controlled access to information system output devices to prevent unauthorized access to Canada's data; e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; f) escorting visitors and monitoring visitor activity; g) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	The Supplier must provide documentation that demonstrates how the Software as a Service Provider (and if applicable the Alternative Service Provider) of the proposed Services complies with the requirements in Data Center Facilities Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are used to ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M4	**Personnel Security**	The Supplier of the proposed Commercially Available Public Software as a Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: a) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services; b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment onboarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or on the reliability of Software as a Services hosting GC assets and data	The Supplier must provide documentation that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, process and procedures that are used to grant and maintain the required level of security screening for the Software as a Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required in the Personnel Security Requirements documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M5	**Third Party Assurance**	The Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing information security policies, procedures, and security controls	The Supplier must provide documentation to Canada that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. The Supplier must provide the following industry certifications for the proposed Service to demonstrate compliance: 1) One of the following: (i) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or (ii) AICPA Service Organization Control (SOC) 2 Type II 2) Self-assessment, or assessments by external auditors, of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. Each provided certification and assessment report must: a) Be valid as of the Submission date; b) Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP; c) Identify the current certification date and/or status; d) identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. e) The scope of the report must map to locations and services offered by the proposed Supplier. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and f) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality management system standard. Please note: • Certifications must be provided for all portions of the proposed Service identified • Certifications must be accompanied by assessment reports. • Certifications must be valid and within the 12 months prior to the start of a contract

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M6	**Supply Chain Management**	The Supplier must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, including Cloud Service Providers, etc.) that would provide Canada with the proposed Commercially Available Public Software as a Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Software as a Service Provider of the proposed Commercially Available Public Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Public Software as a Services of the Software as a Service Provider that have been proposed by the Supplier. Please note Suppliers are advised that subsequent procurement Streams may require the Supplier to notify Canada regularly when there are updates to the list of third party suppliers.	The Supplier must provide documentation list of Sub-processors that could be used to perform any part of the Services in providing Canada with the Services. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the scope activities that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the activities required to support the Services. (1) For SaaS, the Contractor must demonstrate that the IaaS/PaaS leveraged by the Services: (a) Supplier Sub-processors have been assessed in accordance with the CCCS guidelines for localized IT security assessments; and (b) Supplier meet the security obligations for Sub-Processors and/or Subcontractors outlined by the Supplier, for the life of the contract. If the Supplier of the proposed Commercially Available Public Software as a Service does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, the Supplier is requested to indicate this in their response to this requirement.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M7	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Public Software as a Service must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within the supply chain.	The Supplier must demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in Supply Chain Risk Management Requirements as documented under the Software as a Service Provider Information Technology Security Assessment program. To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Software as a Service Provider's approach to SCRM and demonstrate how the Supplier of the proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks

M8	**Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrate how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services; (b) Restrict and minimize access to the Services and Canada's Data's to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Canada's Data's; (d) Constrain all access to service interfaces that host Assets and Canada's Data's to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; (h) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets;	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The substantiation required for the Privileged Access Management documentation, cannot simply be a repetition of the mandatory requirement but must explain and demonstrate and indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers., on how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
		(j) Access controls on objects in storage and granular authorization policies to allow or limit access (k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M9	**Federation of Identity**	**Federation of Identity** The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and (c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity. The substantiation required for in the Federation of Identity cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M10	**Endpoint Protection**	**Endpoint Protection** The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection. The substantiation required for in the Endpoint Protection the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M11	**Secure Development**	**Secure Development** The Supplier must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development. The substantiation required for in the Secure Development, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M12	**Supplier Remote Management**	**Supplier Remote Management** The Supplier must manage and monitor remote administration of the Supplier's Service that are used to host GC services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points; (d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; (e) Authorize remote execution of privileged commands and remote access to security-relevant information.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Supplier Remote Management The substantiation required for in the Supplier Remote Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M13	Information Spillage	**Information Spillage** (1) The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process to isolate and eradicate a contaminated Asset or System; and (c) A process for identifying Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier's information spillage process.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage. The substantiation required for in the Information Spillage, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M14	Cryptographic Protection	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection The substantiation required for in the Cryptographic Protection, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M15	**Data Segregation**	The Supplier must, for both Tiers, implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and **(b)** (b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.

APPENDIX M, PERIODIC USAGE REPORT

(see attached)

APPENDIX N, VENDOR INFORMATION AND AUTHORIZATION FORM

Vendor Name and Address

_____

_____

_____

_____

Legal Status (incorporated, registered, etc.)
☐ **Individual (Sole proprietor)**
☐ **Privately owned corporation**
☐ **Joint Venture or Corporate entity**
☐ **Other (specify):**

_____

GST or HST Registration Number and Business Number (Revenue Canada)

_____

Name and Title of Person authorized to sign on behalf of Vendor

Print Name _____ **Title** _____

Signature _____ **Date** _____

Central Point of Contact

The Vendor has designated the following individual as a central point of contact for all matters pertaining to the proposed contract, including the provision of all information that may be requested:

Name and Title_____

Telephone _____ **Fax** _____

Email _____

Each proposal must include a copy of this page properly completed and signed.

Appendix O - Application for Registration (AFR) for Canadian Entities

See attachment