RETURN BID TO/ RETOURNER LES SOUMISSIONS À :

receptionsoumission-bidsreceiving.spp@international.gc.ca

Department of Foreign Affairs, Trade and Development (DFATD)
Ministère des Affaires étrangères, commerce et développement (MAECD)

Request for Proposal
Demande de proposition
proposal to: Department of Foreign Affairs Trade and Development.

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

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

Comments — Commentaires:

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT — LE PRÉSENT DOCUMENT COMPORTE UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ

Issuing Office – Bureau de distribution
Foreign Affairs, Trade and Development / Affaires étrangères, commerce et développement
It Contracting Services Unit / Unité des services de contrats TI
200 Promenade du Portage,
Gatineau, QC

Title — Sujet SaaS Omnichannel Communication Platform	
Solicitation No. — Nº de l'invitation **23-222062**	Date: **February 28, 2023**
Solicitation Closes — L'invitation prend fin	Time Zone —Fuseau horaire
At /à: **2:00 PM** On / le **March 10, 2023**	EDT (Eastern Daylight Saving Time)
F.O.B. — F.A.B. **Plant-Usine:** ☐ **Destination: X** **Other — Autre:** ☐	
Address Enquiries to — Addresser toutes questions à: Name : Stephen Brown E-Mail: Stephen.Brown@international.gc.ca	
Telephone No. – No de téléphone: **(343) 203-1305**	FAX No. – No de télécopieur :
Destination of Goods and or Services/Destination – des biens et ou services: Department of Foreign Affairs, Trade and Development (DFATD)/**Ministère des Affaires étrangères, commerce et développement (MAECD)**	
Vendor/Firm Name and Address — Raison sociale et adresse du fournisseur/de l'entrepreneur:	
Telephone No. – No de téléphone:	FAX No. – No de télécopieur:
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) — Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur (taper ou écrire en caractères d'imprimerie) _____ _____ Signature Date	

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

Part 5 Certifications 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.

The Annexes include the Statement of Work, the Basis of Payment, the Security Requirements Checklist, the Electronic Payment Instruments, the Federal Contractors Program for Employment Equity - Certification, and any other annexes.

1.2 Summary

1.2.1 The Emergency Watch and Response Centre (EWRC) is Global Affairs Canada's 24/7 365 Day communication hub that provides consular services to Canadian citizens in need of routine or emergency assistance outside of Canada.

Global Affairs Canada requires a Vendor to provide access up to thirty (30) seats to a web-based SaaS integrated communications platform that will integrate the most popular global chat applications. At a minimum the following communication channels must be integrated into the platform: SMS, WhatsApp, live chat (website integrations).

The online platform must have capability to deploy artificial intelligence / machine learning tools, such as chat bots, that integrate with all communication channels. Chat bots, as well as any client facing interface within the control of the vendor, must be available in English and French.

The period of the contract will be from contract award date until one (1) year later plus four (4) one-year irrevocable options allowing Canada to extend the term of the contract.

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

1.2.3 The Federal Contractors Program (FCP) for employment equity applies to this procurement; refer to Part 5 – Certifications and Additional Information, Part 7 - Resulting Contract Clauses and the annex titled Federal Contractors Program for Employment Equity - Certification.

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 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

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

The 2003 (2022-03-29) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

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

Delete: 60 days
Insert: 90 days

2.2 Submission of Bids

Bids must be submitted only to Global Affairs Canada (GAC) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

GAC Bid Receiving Unit in the National Capital Region (NCR) email address is:

receptionsoumission-bidsreceiving.spp@international.gc.ca

2.3 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: 2019-01 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.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than 7 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 question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 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.

2.6 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 favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least 5 days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Bid Challenge and Recourse Mechanisms

(a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

(b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

- Office of the Procurement Ombudsman (OPO)
- Canadian International Trade Tribunal (CITT)

(c) Suppliers should note that there are **strict deadlines** for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

The bid must be gathered per section and separated as follows:

Section I: Technical Bid
Section II: Financial Bid
Section III: Certifications

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

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

Section I: Technical Bid (1 Electronic copy via email)

Section II: Financial Bid (1 Electronic copy via email)

Section III: Certifications (1 Electronic copy via email)

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 hard copy of their bid:

(a) use 8.5 x 11 inch (216 mm x 279 mm) paper.
(b) use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32573). To assist Canada in reaching its objectives, bidders should:

1) Include all environmental certification(s) relevant to your organization (e.g., ISO 14001, Leadership in Energy and Environmental Design (LEED), Carbon Disclosure Project, etc.)
2) Include all environmental certification(s) or Environmental Product Declaration(s) (EPD) specific to your product/service (e.g., Forest Stewardship Council (FSC), ENERGYSTAR, etc.)
3) Unless otherwise noted, bidders are encouraged to submit bids electronically. If hard copies are required, bidders should:
    a. use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably managed forest and containing minimum 30% recycled content; and
    b. use an environmentally preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of Cerlox, duo tangs or binders.

Section I: Technical Bid

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

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

Section II: Financial Bid

3.1.1 Bidders must submit their financial bid in accordance with the Basis of Payment in Annex B.

3.1.2 Electronic Payment of Invoices – Bid

If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Annex “E” Electronic Payment Instruments, to identify which ones are accepted.

If Annex “E” Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices.

Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

3.1.3 Exchange Rate Fluctuation

C3011T (*2013-11-06*), Exchange Rate Fluctuation

The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.

3.1.4 *SACC Manual* Clauses

Section III: Certifications

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

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 evaluation criteria.

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

4.1.1 Technical Evaluation

Mandatory and point rated technical evaluation criteria are included in Attachment 4.1.

4.1.2 Financial Evaluation

4.1.2.1 Mandatory Financial Criteria

SACC Manual Clause A0222T (2014-06-26), Evaluation of Price-Canadian/Foreign Bidders

1. The price of the bid will be evaluated as follows:

   a. Canadian-based bidders must submit firm prices, Canadian customs duties and excise taxes included, and Applicable Taxes excluded.

   b. foreign-based bidders must submit firm prices, Canadian customs duties, excise taxes and Applicable Taxes excluded. Canadian customs duties and excise taxes payable by Canada will be added, for evaluation purposes only, to the prices submitted by foreign-based bidders.

2. Unless the bid solicitation specifically requires bids to be submitted in Canadian currency, bids submitted in foreign currency will be converted to Canadian currency for evaluation purposes. The rate given by the Bank of Canada in effect on the bid solicitation closing date, or on another date specified in the bid solicitation, will be applied as a conversion factor to the bids submitted in foreign currency.

3. Although Canada reserves the right to award the Contract either on an FOB plant or FOB destination, Canada requests that bidders provide prices FOB their plant or shipping point and FOB destination. Bids will be assessed on an FOB destination basis.

4. For the purpose of the bid solicitation, bidders with an address in Canada are considered Canadian-based bidders and bidders with an address outside of Canada are considered foreign-based bidders.

4.2 Basis of Selection

1. To be declared responsive, a bid must:
   a. comply with all the requirements of the bid solicitation; and
   b. meet all mandatory criteria; and
   c. obtain the required minimum points specified for the technical evaluations, and
2. Bids not meeting choose (a) or (b) or (c)" OR will be declared non-responsive.
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. 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%.
5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30%.
6. For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.
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 equals 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating of Technical Merit (70%) and Price (30%)			
Bidder	**Bidder 1**	**Bidder 2**	**Bidder 3**
Overall Score for all the Point Rated Technical Criteria	OS1: 120/135	OS2: 98/135	OS3: 82/135
Bid Evaluated Price	P1: C$60,000.00	P2: C$55,000.00	LP and P3: $50,000.00
Calculations	**Technical Merit Score (OS1 X70)**	**Pricing Score (LP/P1 X 30)**	**Combined Rating**
Bidder 1	120/135 x 70 = 62.22	50/60 x 30 = 24.99	87.21
Bidder 2	98/135 x 70 = 50.81	50/55 x 30 = 27.27	78.08
Bidder 3	82/135 x 70 = 42.51	50/50 x 30 = 30.00	72.51

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 made knowingly or unknowingly, 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 (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the procurement process.

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 (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 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 page of the Employment and Social Development Canada (ESDC) - Labour's website.

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 titled 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.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

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

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

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

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

2. Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

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

PART 7 - RESULTING CONTRACT CLAUSES

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

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex "A" and the Contractor's technical bid entitled _____, dated _____.

7.1.1 Optional Goods and/or Services

The Contracting Authority may exercise the option at any time before the expiry of the Contract by sending a written notice to the Contractor.

7.2 Standard Clauses and Conditions

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

7.2.1 General Conditions

2035 (2022-05-12), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

7.2.2 Supplemental General Conditions

N0004C (2020-05-08), apply to and form part of the Contract.

- **First Party Liability**

  Contract Performance: The Contractor is fully liable for all damages to Canada, arising from the Contractor's performance or failure to perform the Contract.

  Data Breach: The Contractor is fully liable for all damages to Canada resulting from its breach of security or confidentiality obligations resulting in unauthorized access to or unauthorized disclosure of records or data or information owned by Canada or a third party.

  Limitation Per Incident: Subject to the following section, irrespective of the basis or the nature of the claim, the Contractor's total liability per incident will not exceed the cumulative value of the Contract invoices for 12 months preceding the incident.

  No Limitation: The above limitation of Contractor liability does not apply to:

  a. wilful misconduct or deliberate acts of wrongdoing, and

  b. any breach of warranty obligations.

  Third Party Liability: Regardless whether the third party claims against Canada, the Contractor or both, each Party agrees that it will accept full liability for damages that it causes to the third party in connection with the Contract. The apportionment of liability will be the amount set out by agreement of the Parties or determined by a court. The Parties agree to reimburse each other for any payment to a third party in respect of damages caused by the other, the other Party agrees to promptly reimburse for its share of the liability.

7.3 Security Requirements

Security is further detailed in Annex C, Security Requirements Checklist and Annex D.

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from date of Contract to one year later inclusive.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 4 additional 1 year period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least 30 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Stephen Brown
Title: Procurement Officer I agent d'approvisionnement
Email: stephen.brown@international.gc.ca
D. 343-203-1305 C: 613-885-5351
200 Prom. du Portage, Gatineau, QC, K1A-0G4
Global Affairs Canada I Affaires mondiales Canada
Government of Canada I Gouvernement du Canada

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.

7.5.2 Project Authority

The Project Authority for the Contract is: (to be inserted at contract award)

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.

7.5.3 Contractor's Representative

(to be inserted at contract award)

7.6 Proactive Disclosure of Contracts 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: 2019-01 of the Treasury Board Secretariat of Canada.

7.7 Payment

7.7.1 Basis of Payment

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm price as specified in Annex B. Customs duties are excluded 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.

7.7.2 Limitation of Expenditure

1. Canada's total liability to the Contractor under the Contract must not exceed the amount indicated on the front page of the Contract. 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% committed, or

b. four 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.

7.7.3 Method of Payment – Single Payment

Canada will pay the Contractor upon completion and delivery of the Work 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.

7.7.4 Electronic Payment of Invoices – Contract

The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s): (to be completed at contract award)

a. Direct Deposit (Domestic and International);

7.8 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.

2. One (1) copy must be forwarded to the Contracting Authority identified under the section entitled "Authorities" of the Contract.

7.9 Certifications and Additional Information

7.9.1 Compliance

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.

7.10 Applicable Laws

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

7.11 Priority of Documents

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

(a) the Articles of Agreement;
(b) the supplemental general conditions N0004C (2020-05-08);
(c) the general conditions 2035 (2022-05-12), General Conditions - Higher Complexity – Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirement Check List;
(g) Annex D, IT Security Requirements Technical Annex
(h) Annex E. Electronic Payment Instrument;
(i) Annex F, Federal Contractors Program for Employment Equity – Certification;
(j) Attachment 4.1, Bid Evaluation Criteria;
(k) the Contractor's bid dated _____, (*insert date of bid*) (*If the bid was clarified or amended, insert at the time of contract award:*", as clarified on _____" ***or*** ",as amended on _____" *and insert date(s) of clarification(s) or amendment(s))* including its Inuit Benefits Plan. (*if applicable*).

7.12 Foreign Nationals (Canadian Contractor *OR* Foreign Contractor)

SACC Manual clause A2000C (2006-06-15) Foreign Nationals (Canadian Contractor)

OR

SACC Manual clause A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

7.13 Insurance or Insurance Requirements

SACC Manual clause G1005C (2016-01-28) Insurance - No Specific Requirement

7.14 Limitation of Liability – Public Cloud Software as a Service (SaaS) N0004C

- **First Party Liability**
    - **Contract Performance:** The Contractor is fully liable for all damages to Canada, arising from the Contractor's performance or failure to perform the Contract.
    - **Data Breach:** The Contractor is fully liable for all damages to Canada resulting from its breach of security or confidentiality obligations resulting in unauthorized access to or unauthorized disclosure of records or data or information owned by Canada or a third party.

- **Limitation Per Incident:** Subject to the following section, irrespective of the basis or the nature of the claim, the Contractor's total liability per incident will not exceed the cumulative value of the Contract invoices for 12 months preceding the incident.
- **No Limitation:** The above limitation of Contractor liability does not apply to:
  a. wilful misconduct or deliberate acts of wrongdoing, and
  b. any breach of warranty obligations.

- **Third Party Liability:** Regardless whether the third party claims against Canada, the Contractor or both, each Party agrees that it will accept full liability for damages that it causes to the third party in connection with the Contract. The apportionment of liability will be the amount set out by agreement of the Parties or determined by a court. The Parties agree to reimburse each other for any payment to a third party in respect of damages caused by the other, the other Party agrees to promptly reimburse for its share of the liability.

7.15 Dispute Resolution

(a) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.

(b) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.

(c) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.

(d) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

ANNEX "A", STATEMENT OF WORK

1. Objective

The objective of this RFP is to identify a commercial vendor to provide a Software-as-a-Service omnichannel communications platform for use by the Emergency Watch and Response Centre of Global Affairs Canada.

2. Background

The Emergency Watch and Response Centre (EWRC) is Global Affairs Canada's 24/7 and 365 Day communications hub that provides consular services to Canadians citizens in need of routine or emergency assistance outside of Canada.

During emergency situations, such as the COVID-19 Global Repatriation Operation, enquiries to the EWRC can exceed 500 enquiries / hours. As a workflow management strategy, the EWRC intends to leverage artificial intelligence, machine learning, and natural language processing to automate responses to routine enquiries originating from chat applications and/or live chat capability embedded in departmental websites.

Prior to 2021, Canadians in distress overseas could contact the EWRC via telephone, fax, SMS, or e-mail. In 2021, a pilot project was undertaken to introduce additional communications channels, including live chat and WhatsApp. The pilot project delivered a web-based software-as-a-service platform integrating live chat, WhatsApp, and SMS into a unified engagement hub. The pilot project platform had the ability to integrate additional social media and chat app channels, and leveraged advanced workflow management tools using artificial intelligence, machine learning, and natural language processing.

3. Scope

The vendor must provide access of up to thirty (30) seats to a web-based SaaS integrated communications platform that will integrate the most popular global chat applications. At a minimum the following communications channels must be integrated into the platform: SMS, WhatsApp, live chat (website integrations).

The online platform must have capability to deploy artificial intelligence / machine learning tools, such as chat bots, that integrate with all communications channels. Chat bots, as well as any client facing interfaces within the control of the vendor, must be available in English and French.,

The platform must provide tools for:

- Managerial supervision and support such as chat session monitoring and transcript reviews.
- Data analysis and analytics
- Workflow automations, such as message routing, queue management, and triggers and automated responses.
- Third part integrations, specifically with Microsoft Dynamics 365.
- Knowledge bases (ideally predictive knowledge bases) that support agent responses with information recommendations and/or pre-determined response suggestions.

4. Exclusions

Incoming voice calls routed through the Global Affairs Canada PBX system will not be processed through the omnichannel communications platform. However, the omnichannel communications platform should be able to handle voice communications routed through a chat app.

The vendor is not required to obtain / create chat application accounts on behalf of Global Affairs Canada.

5. Technical Specifications

The tool must:

Be delivered through a software-as-a-service model.
Incorporate all communications channels into a single engagement hub.
Incorporate, at a minimum, the following communication channels: SMS, WhatsApp, live chat.
Be able to onboard and offboard new channels in response to shifting usage patterns of social media and chat applications.
Incorporate workflow automation tools, such as standardized response messaging, automated response messages, message routing, etc.
Have the ability to export conversation data
Support multiple languages, including English and French
Allows for third-party integration capability with Microsoft Dynamics 365.
Has flexible data retention and disposal framework that can be aligned with Global Affairs Canada's requirements.
Operates with high-level availability and with data centre level redundancy.
Process and store all data in Canada
Meets technical security standards, including ISO/IEC 27001:2013 (also known as ISO 27001), and AICPA SOC 2 Type II.
Provides 24/7 technical support, with appropriate escalation mechanisms, for contact centre agents.

Thirty (30) seats must be provided by the vendor to the client in order to access the online tool.

All client users must be able to access and use the tool simultaneously.

Remote training must cover:

Accessing the tool
Agent use of the tool to communicate the clients
Administrator use of the tool for user management and system configuration
Configuration and use of artificial intelligence / machine learning / natural language processing tools
How to configure and run custom reports / data analytics

6. Travel

Travel will not be required in the execution of this contract. All training and support activities are to be provided remotely.

7. Constraints

Vendor will be required to use their own in-house systems in order to carry out the deliverables, as the vendor will not have direct access to client systems. Government furnished equipment, tool, facilities, etc. will not be necessary for the conduct of this project.

8. Client Support

The client project authority will make him/herself available to the vendor via email or phone as necessary during business hours (09h00 – 17h00 Eastern) during the business week (Monday to Friday) for the duration of the contract to respond to any related inquiries.

9. Deliverables

a. Access for thirty (30) seats for twelve (12) months on an online SaaS omnichannel communications platform that must be operational and accessible by the client as of the contract start date;
b. Training sessions covering full use of the tool; and
c. Ongoing technical support

ANNEX "B", BASIS OF PAYMENT

Estimated quantities for evaluation purposes only

Estimated quantities for the contract period

The following estimated quantities will be used for the contract period from January 1, 2023 to December 31, 2023:

Requirement	Unit	Estimated annual volume	Price
Set-up Fee	One time	1	
Monthly fee to include all requirements as stated in the Statement of Work for up to 30 concurrent users including unlimited communications using all communications channels	Per month	12 month	
Training for up to 30 users in the full use of the platform	Per hour	10 hours	

Estimated quantities for the option periods

Option Year One – January 1, 2024 to December 31, 2024

Requirement	Unit	Estimated annual volume	Price
Monthly fee to include all requirements as stated in the Statement of Work for up to 30 concurrent users including unlimited communications using all communications channels	Per month	12 month	
Training for up to 30 users in the full use of the platform	Per hour	10 hours	

Option Year Two - January 1, 2025 to December 31, 2025

Requirement	Unit	Estimated annual volume	Price
Monthly fee to include all requirements as stated in the Statement of Work for up to 30 concurrent users including unlimited communications using all communications channels	Per month	12 month	
Training for up to 30 users in the full use of the platform	Per hour	10 hours	

Option Year 3 – January 1, 2026 to December 31, 2026

Requirement	Unit	Estimated annual volume	Price
Monthly fee to include all requirements as stated in the Statement of Work for up to 30 concurrent users including unlimited communications using all communications channels	Per month	12 month	
Training for up to 30 users in the full use of the platform	Per hour	10 hours	

Option Year 4 – January 1, 2027 to December 31, 2026

Requirement	Unit	Estimated annual volume	Price
Monthly fee to include all requirements as stated in the Statement of Work for up to 30 concurrent users including unlimited communications using all communications channels	Per month	12 month	
Training for up to 30 users in the full use of the platform	Per hour	10 hours	

ANNEX "C", SECURITY REQUIREMENTS CHECK LIST

Government of Canada / Gouvernement du Canada

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

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
Global Affairs Canada	CSW/CSD/CFM

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

Comm100 Enterprise Platform subscription providing a software-as-a-service chat application platform to support COVID-19 response.

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) ☐

Security Classification / Classification de sécurité

TBS/SCT 350-103 (2004/12)

Canada

Government of Canada | Gouvernement du Canada

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

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?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité : ☑ No Non ☐ Yes Oui

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: Unclass
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

Government of Canada / Gouvernement du Canada

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential / Confidentiel	Secret	Top Secret / Très Secret	NATO Restricted / NATO Diffusion Restreinte	NATO Confidential / NATO Confidentiel	NATO Secret	COSMIC Top Secret / COSMIC Très Secret	Protected / Protégé A	Protected / Protégé B	Protected / Protégé C	Confidential / Confidentiel	Secret	Top Secret / Très Secret
Information / Assets / Renseignements / Biens	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Production	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Media / Support TI	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Link / Lien électronique	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

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

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

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

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

ANNEX "D", IT Security Requirements Technical Annex

(for processing, producing, or storing sensitive information up to PROTECTED A in the cloud)

GLOBAL AFFAIRS CANADA (GAC)

RATIONALE

THE FOLLOWING IT SECURITY ANNEX HAS BEEN DESIGNED SPECIFICALLY FOR REQUESTS FOR PROPOSALS (RFPS) THAT WILL PROCESS, PRODUCE, OR STORE GAC INFORMATION IN THE CLOUD THROUGH A CLOUD SERVICE PROVIDER (CSP) SOLUTION.

THIS IT SECURITY ANNEX IS INTENDED FOR INFORMATION THAT HAS BEEN CATEGORIZED UP TO **PROTECTED A**.

1.0 INTRODUCTION

FURTHER TO THE SECURITY REQUIREMENTS CHECKLIST (SRCL), THIS ANNEX WILL DESCRIBE THE SECURITY REQUIREMENTS FOR THE PROTECTION OF **PROTECTED A** INFORMATION PRODUCED, PROCESSED, OR STORED UNDER THE TERMS OF THIS CONTRACT, INCLUDING:

A) CONTRACTOR'S INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY (IM/IT) SYSTEMS USED FOR PROCESSING, PRODUCING, TRANSMITTING OR STORAGE OF **PROTECTED A** INFORMATION;
B) CLOUD SERVICE BROKER/CLOUD BROKER (CSB) IM/IT SYSTEMS USED FOR PROCESSING, PRODUCING, TRANSMITTING OR STORAGE OF **PROTECTED A** INFORMATION; AND
C) 3RD PARTY CLOUD SERVICE PROVIDER/CLOUD SOLUTION PROVIDER (CSP) INFRASTRUCTURE AS A SERVICE (IAAS), PLATFORM AS A SERVICE (PAAS) AND SOFTWARE AS A SERVICE (SAAS) LAYERS USED IN THE PROVISION OF SERVICES UNDER THE TERMS OF THIS CONTRACT.

UNAUTHORIZED DISCLOSURE OF **PROTECTED A** INFORMATION COULD CAUSE INJURY TO AN INDIVIDUAL, ORGANIZATION OR GOVERNMENT. AS SUCH, GAC AND CONTRACTOR AGREE TO MAXIMIZE THE SECURITY OF THE SOLUTION ACCORDING TO TERMS IDENTIFIED IN THIS TECHNICAL SECURITY ANNEX.

2.0 CERTIFICATIONS

2.1 THE CONTRACTOR MUST DEMONSTRATE, PRIOR TO CONTRACT AWARD, THAT THE CSP HAS RECEIVED **AT LEAST ONE** OF THE FOLLOWING INDUSTRY THIRD-PARTY CERTIFICATIONS[1]:

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) 27001;

OR

[1] FedRAMP, "Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) Level 2", Payment Card Industry Data Security Standard (PCI DSS), and other certifications may be considered during the assessment but will not replace the third-party certifications mentioned here.

- AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA) SERVICE ORGANIZATION CONTROLS (SOC) TYPE II.

2.2 THE CONTRACTOR MUST DEMONSTRATE, PRIOR TO CONTRACT AWARD, THAT THE CSP HAS PERFORMED A SELF-ASSESSMENT TO CSA CLOUD CONTROLS MATRIX, ALSO KNOWN AS *CLOUD SECURITY ALLIANCE (CSA) SECURITY, TRUST AND ASSURANCE REGISTRY (STAR) LEVEL 1*. A *CLOUD SECURITY ALLIANCE (CSA) SECURITY, TRUST AND ASSURANCE REGISTRY (STAR) LEVEL 2* CAN BE ACCEPTED AS A SUBSTITUTE.

2.3 THE CONTRACTOR MUST ENSURE THAT THE CERTIFICATIONS USED TO COMPLY WITH THE CLOUD SERVICE PROVIDER SECURITY REQUIREMENTS ARE MAINTAINED AND VALID FOR THE DURATION OF THE CONTRACT. THE CONTRACTOR MUST ALSO STIPULATE IF THE CERTIFICATION OR AUDIT STANDARD APPLIES TO THE WHOLE SOLUTION OR TO A SPECIFIED PORTION OF THEIR SOLUTION.

2.4 THE CONTRACTOR MUST PROVIDE PROOF OF ITS SECURITY CERTIFICATION(S) AND ALL APPLICABLE AUDIT STANDARDS FOR ITS PROPOSED SOLUTION IN THE FORM OF A VALID CERTIFICATE OR AUDIT STANDARD AND DESCRIBE HOW THE CERTIFICATION OR AUDIT STANDARD WAS ASSESSED AND OBTAINED (I.E. THIRD-PARTY INDUSTRY CERTIFICATIONS OR AUDIT REPORTS) FOR EACH CERTIFICATION AND AUDIT STANDARD HELD. A THIRD-PARTY CERTIFICATION REQUIRES AN INDEPENDENT THIRD PARTY THAT IS BOUND TO BE OBJECTIVE AND TO APPLY PROFESSIONAL STANDARDS TO THE EVIDENCE IT REVIEWS AND PRODUCE.

3.0 SECURITY REQUIREMENTS AND TRACEABILITY

DEPARTMENTS REQUIRE GRADUATED SAFEGUARDS THAT ARE COMMENSURATE WITH THE RISKS TO THEIR INFORMATION AND IT ASSETS. SECURITY CONTROL PROFILES ARE ESTABLISHED IN SUPPORT OF THIS REQUIREMENT.

A BASELINE SECURITY CONTROL PROFILE IS A SET OF IT SECURITY CONTROLS THAT AN ORGANIZATION ESTABLISHES AS MINIMUM MANDATORY REQUIREMENTS FOR ITS INFORMATION SYSTEMS. BY ADHERING TO A STANDARDIZED SET OF SECURITY CONTROLS, DEPARTMENTS CAN:

- IDENTIFY AND ASSESS RISKS;
- DEVELOP STRATEGIES TO APPROPRIATELY MITIGATE RISKS.

COMMUNICATIONS SECURITY ESTABLISHMENT (CSE) IT SECURITY GUIDANCE 33 (ITSG-33)[2] CONTAINS DEFINITIONS OF SECURITY CONTROLS THAT GAC USES AS A FOUNDATION FOR THE PROTECTION OF GOVERNMENT OF CANADA (GC) INFORMATION SYSTEMS AND MANAGING INFORMATION TECHNOLOGY (IT) SECURITY RISKS. FAMILIARITY WITH ITSG-33 TERMINOLOGY[3] AND SPECIFICALLY, THE CONTROLS DESCRIBED IN ANNEX 3A – SECURITY CONTROL CATALOGUE[4] WILL BE BENEFICIAL IN DIALOGUE WITH GAC SECURITY PRACTITIONERS WHO WILL BE INVOLVED DURING THE DEVELOPMENT AND ASSESSMENT OF THE SOLUTION.

[2] https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33
[3] https://cyber.gc.ca/en/guidance/annex-5-glossary-itsg-33
[4] https://cyber.gc.ca/en/guidance/annex-3a-security-control-catalogue-itsg-33

THE GOVERNMENT OF CANADA SECURITY CONTROL PROFILE FOR CLOUD-BASED GC IT SERVICES SETS OUT THE BASELINE SECURITY CONTROLS RECOMMENDED FOR IMPLEMENTATION BY CSPS AND GC DEPARTMENTS IN ORDER TO APPROPRIATELY PROTECT CLOUD-BASED SERVICES THAT HAVE A SECURITY CATEGORY OF **PROTECTED A**.

3.1 THE CONTRACTOR MUST WORK WITH GAC SECURITY PRACTITIONERS TO IDENTIFY, UNDERSTAND AND DOCUMENT THE RISKS FACING THE APPLICATION. THE PURPOSE OF THIS EFFORT IS TO IDENTIFY THE KEY RISKS TO THE IMPORTANT ASSETS AND FUNCTIONS PROVIDED BY THE APPLICATION, AND TO ESTABLISH A BASIS FOR THE SELECTION AND TAILORING OF THE SET OF BASELINE SECURITY CONTROLS IDENTIFIED IN THE **GLOBAL AFFAIRS CANADA SECURITY CONTROL PROFILE FOR CLOUD-BASED GC IT SERVICES** PROVIDED BY TBS (*TBS PLAYBOOK FOR SAAS APPLICATIONS UP TO PROTECTED B* SRTM). PROVIDE THE INFOBANK DOCUMENT **#14310732** TO BIDDERS, AS REQUESTED.

3.2 THE CONTRACTOR IS RESPONSIBLE FOR MEETING ALL SECURITY REQUIREMENTS IDENTIFIED WITH A "YES" IN THE "TBS PLAYBOOK PBMM CONTROLS" COLUMN OF THE **GLOBAL AFFAIRS CANADA SECURITY CONTROL PROFILE FOR CLOUD-BASED GC IT SERVICES**. SOME CONTROLS MAY BE EXCLUDED AS PART OF THE TAILORING PROCESS. EXCLUDING SECURITY CONTROLS WILL DEPEND UPON THE THREATS AND RISKS IDENTIFIED WITH PROPOSED SOLUTION AND DATA CLASSIFICATION.

3.3 THE CONTRACTOR MUST COLLABORATE WITH GAC SECURITY PRACTITIONERS IN THE TAILORING OF DETAILED SECURITY REQUIREMENTS TO ACHIEVE ACCEPTABLE RISK AS A PART OF THE SPECIFICATION OF THE SOLUTION. SECURITY REQUIREMENTS MAY BE SATISFIED BY INDUSTRY CERTIFICATIONS (SEE SECTION *2.0 CERTIFICATIONS*), CUSTOM SOFTWARE, THIRD PARTY SOFTWARE, PLATFORM AND/OR INFRASTRUCTURE COMPONENTS. THE TAILORED VERSION OF THE **GLOBAL AFFAIRS CANADA SECURITY CONTROL PROFILE FOR CLOUD-BASED GC IT SERVICES** SHALL BECOME AND BE KNOWN AS THE **SECURITY REQUIREMENTS TRACEABILITY MATRIX** (**SRTM**)**.**

3.4 THE CONTRACTOR MUST IDENTIFY AND TRACE SECURITY CONTROLS THAT ARE SATISFIED THROUGH ANY CERTIFICATIONS (SEE SECTION *2.0 CERTIFICATIONS*) WITHIN THE SRTM. THE CONTRACTOR MUST DOCUMENT AND PROVIDE ASSURANCE FOR ALL OTHER SECURITY CONTROLS DETERMINED TO BE IN-SCOPE BY THE TAILORING PROCESS, ACCORDING TO THE SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) PROCESS (SEE SECTION 15.0 *SECURITY ASSESSMENT AND AUTHORIZATION (SA&A)*).

3.5 IN ACCORDANCE WITH THE SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) (SEE SECTION 15.0 *SECURITY ASSESSMENT AND AUTHORIZATION (SA&A)*), THE CONTRACTOR MUST PROVIDE DOCUMENTATION THAT CLEARLY EXPLAINS THE DESIGN THAT WILL MEET EACH OF THE SECURITY REQUIREMENTS. IN MOST CASES, THIS DOCUMENTATION WILL DESCRIBE SECURITY MECHANISMS, WHERE THE MECHANISMS FIT INTO THE ARCHITECTURE AND ALL RELEVANT DESIGN PATTERNS TO ENSURE THEIR PROPER USE. THE DESIGN MUST CLEARLY SPECIFY WHETHER THE SUPPORT COMES FROM CUSTOM SOFTWARE, THIRD PARTY SOFTWARE, THE PLATFORM, OR THE INFRASTRUCTURE.

4.0 PERSONNEL REQUIREMENTS

4.1 SECURITY ARCHITECT ROLE

4.1.1 THE CONTRACTOR MUST ASSIGN RESPONSIBILITY FOR SECURITY TO A SINGLE SENIOR TECHNICAL RESOURCE, TO BE KNOWN AS THE SECURITY ARCHITECT. THE SECURITY ARCHITECT MUST CERTIFY THE SECURITY OF EACH DELIVERABLE. THE CERTIFICATION SHALL BE IDENTIFIED AS THE "SECURITY CERTIFICATION PACKAGE".

4.2 OPERATIONAL SUPPORT PERSONNEL REQUIREMENTS

4.2.1 CITIZENSHIP AND RESIDENCE

4.2.1.1 ALL CONTRACTOR SERVICE DESK, SOC AND NOC OPERATIONAL STAFF FOR THE ENTIRE VENDOR SOLUTION SHOULD BE CITIZENS OF CANADA AND/OR COUNTRIES WITH WHICH CANADA HAS NEGOTIATED INTERNATIONAL BILATERAL SECURITY INSTRUMENTS (IBSI)[5], OR EUROPEAN UNION AND/OR NATO COUNTRIES.

4.2.1.2 ALL CONTRACTOR SERVICE DESK, SOC AND NOC OPERATIONAL STAFF FOR THE ENTIRE VENDOR SOLUTION SHOULD RESIDE IN CANADA OR WITHIN COUNTRIES WITH WHICH CANADA HAS NEGOTIATED IBSI OR WITHIN EUROPEAN UNION OR WITHIN NATO COUNTRIES.

4.2.2 Background Investigations

4.2.2.1 The Contractor must provide proof of the reliability of all Operational personnel who perform administrative functions for the proposed solution through a documented security screening process. Security screening must require either:

a) Proof of a Public Services and Procurement Canada (PSPC) "reliability status"; or
b) Self-assessment for a Contractor equivalent process that includes a 5-year background check, including:
   (i) Verification of identity requiring a minimum of two instances of evidence of identity, one of which must be foundational evidence of identity (i.e., a government issued identity artefact, such as birth certificate, passport or driver's license);
   (ii) Criminal record check; and
   (iii) Credit check.

4.2.2.2 Any candidate or existing Operational personnel who have an accusation before court **are not acceptable** candidates until any criminal charges are resolved. On demand, the Contractor must supply documentation reflecting favorable adjudication of background investigations for all personnel supporting the system.

5.0 Operations Centres

[5] https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html, International security instruments Section

5.1 The Security Operations Centre (SOC), Network Operations Centre (NOC) and Service Desk should be physically located and operate within Canada, countries with which Canada has IBSI, or within countries belonging to EU or NATO.

6.0 Compliance with Security Policy Implementation Notice (SPIN)

6.1 TBS Direction on the Secure Use of Commercial Cloud Services (SPIN 2017-01)

6.1.1 In accordance with the TBS Direction on the Secure Use of Commercial Cloud Services[6], the Contractor must ensure that:

a) The solution enables the identification and authentication of individuals and devices to an appropriate level of assurance before being granted access to information and services hosted in cloud services. Such authentication is in accordance with the Standard on Identity and Credential Assurance[7] and aligns with GC enterprise identity and authentication services.

b) Access is restricted to personnel based on the principles of least privilege, need to know and segregation of duties, and is supported through appropriate security controls. Restricting access includes:
   (i) establishing appropriate use restrictions and device configurations;
   (ii) taking into consideration the threat environment when accessing cloud services.

c) Privileged user access to cloud-based services implements stronger authentication mechanisms (multi-factor authentication) adhering to CSE IT Security Guidance for Practitioners (ITSP).30.031 V3[8] must be configured. Additional security measures, such as the use of privileged access workstations and dedicated management networks, may also be required to further mitigate the risks associated with privileged access.

d) Data transiting networks must be adequately protected through the use of appropriate encryption and network safeguards. Cloud-based services must make use of CSE-approved cryptographic algorithms and protocols, as outlined in:
   - CSE's ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information;
   - CSE's ITSP.40.062 Guidance on Securely Configuring Network Protocols.

e) Robust key management processes and procedures are implemented to protect encryption keys from being compromised or lost, which could result in unauthorized disclosure or loss of information.

f) All external interfaces of the cloud-based service must be identified and appropriately protected.

g) CSPs clearly document the security controls and features implemented within their cloud services to help the GC understand the security controls within its scope of responsibility. Such controls include those inherited by the CSP. For example, a software provider using an infrastructure provider to deliver a Software as a Service (SaaS) offering will inherit security controls from the infrastructure provider. In this case, the CSP is expected to obtain assurance that the underlying infrastructure as a service (IaaS) or platform as a service (PaaS) offering being leveraged for the SaaS offering has:
   - implemented the appropriate controls within its scope;

[6] https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html
[7] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776
[8] https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3

- obtained valid third-party industry certifications or audit reports.

h) Departments are required to continuously manage vulnerabilities in information systems. These measures extend to CSPs for the cloud service components within their scope of responsibility.

i) CSPs are expected to notify the GC when a security incident or breach of GC data or their cloud services impacts the cloud-based GC service. Such notifications should be distributed to:
   - relevant departmental contacts (for example, cloud-based service owner);
   - Canadian Centre for Cyber Security (CCCS).

7.0 Compliance with IT Policy Implementation Notice (ITPIN)

7.1 TBS Direction for Electronic Data Residency (ITPIN 2017-02)

7.1.1 In the spirit of the Treasury Board of Canada Secretariat IT Policy Implementation Notice (ITPIN) 2017-02[9], it is preferred that:

a) All sensitive electronic data that has been categorized as **PROTECTED A** should be stored in a GC-approved computing facility located within the geographic boundaries of Canada.

b) All GC **PROTECTED A** data must be encrypted when in transit outside of GC-controlled Operations and Security Zones within Canada or internationally.

8.0 Secure Code Practice

8.1 The Contractor must follow industry best practices, including but not limited to the following:

a) When developing custom code necessary to satisfy the terms of this contract:

(i) The Contractor agrees to identify and follow a set of secure coding guidelines (such as SAFECode Fundamental Practices for Secure Software Development[10]) when completing deliverables identified in the contract. Guidelines must indicate how code should be formatted, structured, and commented.

(ii) The Contractor agrees to use a set of common security control programming interfaces (such as the OWASP Enterprise Security API (ESAPI)[11]). Common security control programming interfaces must define how security controls must be called and how security controls must function.

(iii) All security-relevant code must be thoroughly commented. All code must be reviewed by at least one other Contractor against the security requirements and coding guideline before it is considered ready for unit test.

[9] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html
[10] https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf
[11] https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

(iv) The software must not include any of the flaws described in the current OWASP Top Ten Web Application Security Risks[12] .

(v) The Contractor warrants that the software shall not contain any code that does not support a software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

(vi) The Contractor must perform application security analysis and testing during the System Development Life Cycle. The Contractor must provide the findings to GAC. The Contractor must remediate security flaws discovered during the design.

(vii) The Contractor must disclose what tools are used in the software development environment to encourage secure coding.

(viii) The Contractor must use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

(ix) The Contractor must use a build process that reliably builds a complete distribution from source. This process must include a method for verifying the integrity of the software delivered to GAC.

(x) The Contractor must disclose all third party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

b) The Contractor must make reasonable efforts to ensure that third party software meets all the terms of this agreement and is as secure as custom developed code developed under this agreement.

9.0 Data Isolation

9.1 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 functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

a) The separation between Contractor's internal administration from resources used by its customers;

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; and

c) Ability for the GC to support isolation within GC-managed tenant environment.

[12] https://owasp.org/www-project-top-ten/

9.2 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.

10.0 Key Management

10.1 The Contractor must provide Canada with a key management service that provides:

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.

11.0 Supply Chain Risk Management

11.1 The Contractor must implement safeguards 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.

12.0 Security Review

12.1 When developing custom code necessary to satisfy the terms of this contract:

12.1.1 GAC has the right to have the software and/or solution reviewed for security flaws at their expense at any time within 60 days of delivery[13]. The Contractor agrees to provide reasonable support to the review team by providing source code and access to test environments.

12.1.2 Security reviews must cover all aspects of the software delivered, including custom code, components, products, and system configuration.

[13] In this document, "*delivery*" is defined as the completion of the terms of the contract for which a GAC *Authority to Operate* (ATO) has been granted, and the Cloud Service Provider (CSP) has committed to any ATO conditions and associated timelines, to GAC satisfaction.

12.1.3 At a minimum, the security review must cover all of the security requirements and should search for other common vulnerabilities. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review.

12.1.4 Security issues uncovered will be reported to both GAC and Contractor. All issues will be tracked and remediated as specified in Section 13.0 *Security Issue Management*.

13.0 Security Issue Management

13.1 The Contractor must manage security issues as follows:

13.1.1 The Contractor will track all security issues uncovered during the entire lifecycle, whether a requirement, design, implementation, testing, deployment, or operational issue. The risk associated with each security issue will be evaluated, documented, and reported to GAC as soon as possible after discovery.

13.1.2 The Contractor will appropriately protect information regarding security issues and associated documentation, to help limit the likelihood that vulnerabilities in operational software are exposed.

13.1.3 Security issues that are identified before delivery must be fixed by the Contractor. Security issues discovered after delivery must be handled in the same manner as other security issues as specified in this technical security annex.

14.0 Assurance

14.1 The Contractor must provide a "Certification Package" consisting of the security documentation created throughout the development, test and implementation process. The Certification Package must include:

a) A project plan that incorporates the GAC Security Assessment and Authorization (SA&A) activities (see Section 15.0 *Security Assessment and Authorization (SA&A)*);
b) Proof of any certificates or audit standards stated to address security requirements (see Section *2.0 Certifications*);
c) A completed Security Requirements Traceability Matrix (SRTM) (see Section 3.0 *Security Requirements and Traceability*);
d) Proof of Personnel Requirements (see Section 4.0 *Personnel Requirements*);
e) Proof of Operations Centre compliance with the requirement (see Section 5.0 *Operations Centres*);
f) Proof of compliance with all GC policies (SPIN) (see Section 6.0 *Compliance with Security Policy Implementation Notice (SPIN)*), in the form of evidence in an SRTM or other suitable documentation;
g) Proof of compliance with all GC policies (ITPIN) (see Section 7.0 *Compliance with IT Policy Implementation Notice (ITPIN)*), in the form of evidence in an SRTM or other suitable documentation;
h) Proof of Contractor best practices, including:

(i) Identification of secure coding guidelines used for any code developed under this contract;
(ii) Identification of source of security control programming interfaces;
(iii) Vulnerability assessment and results, demonstrating that solution software is not susceptible to any flaws described in the OWASP Top Ten Most Critical Web Application Vulnerabilities.

i) Architecture and Design documentation deliverables (see Section 15.0 *Security Assessment and Authorization (SA&A)*), including:
(i) High-Level Security Design;
(ii) Detailed Security Design;
(iii) Security Test Plan;
(iv) Security Test Report;
(v) Vulnerability Assessment (VA) Plan;
(vi) Vulnerability Assessment (VA) Report;
(vii) Security Installation Verification Plan; and/or
(viii) Security Installation Verification Report.

14.2 The package must establish that the security requirements, design, implementation, and test results were properly completed and all security issues were resolved appropriately.

14.3 The Security Architect must certify that the software meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status must be fully documented with the delivery.

14.4 Security Acceptance and Maintenance

14.4.1 Acceptance

14.4.1.1 The solution shall not be considered accepted until the Certification Package is complete and there is assurance that all **PROTECTED A** data will be protected from unauthorized disclosure which could cause serious injury to an individual, business or government.

14.4.1.2 Any other security issues which have not been resolved and which do not jeopardize protection of data must accompany documentation for future implementation. GAC and Contractor agree to scope the effort required to resolve these extra security issues and to negotiate in good faith to achieve an agreement to perform the required work to address them. GAC reserves the right to have outstanding security issues, which do not jeopardize protection of data, addressed by a Task-Based Authorization (TA) if it is deemed that the security issue will take an excessive amount of work to complete.

14.4.2 Investigating and Resolving Security Issues

14.4.2.1 Within 90 days after obtaining a GAC Authority to Operate (ATO), if security issues are discovered or reasonably suspected, Contractor must assist GAC in performing an investigation to determine the nature of the issue. Contractor and GAC agree to scope the effort required to resolve security issues and to negotiate in good faith to achieve an agreement to perform the required work to address them.

14.4.3 Other Security Issues

14.4.3.1 The Contractor must use all commercially reasonable efforts consistent with sound software development practices, taking into account the severity of the risk, to resolve all security issues as quickly as possible.

15.0 Security Assessment and Authorization (SA&A)

GAC has adapted the Information System Security Implementation Process (ISSIP), described in the CSE publication IT Security Risk Management: A Lifecycle Approach (ITSG-33)[14], as a foundation for the GAC Security Assessment and Authorization (SA&A) process. The SA&A process is the mechanism by which risk to an IT system is understood, mitigated and consistently and measurably managed throughout its lifecycle. An Authority to Operate (ATO) is the business owner's approval to allow a project, program, facility, or system to operate using a particular set of safeguards within an acceptable level of residual risk.

The GAC SA&A process (as described in this section) is conducted in **phases** which are intended to promote a "security by design" philosophy. A review point follows each phase. Each successive review point corresponds to an increasing level of detail in the architecture, design, implementation and operational phases of the delivered solution. The purpose of the review is to ensure traceability against security requirements, continuity in the design, and a validation that security mechanisms are both present and adequate.

15.1 The Contractor must comply with, and address all SA&A requirements.

15.2 The Contractor must incorporate the GAC SA&A phases in a project schedule and obtain approval of the project schedule by the GAC Project Authority prior to commencing development work under the contract.

15.3 The Contractor must address all requirements stated in Section 15.5 *Security Assessment and Authorization Requirements* at each phase of the project, according to the approved project schedule.

15.4 The Contractor must submit all deliverables identified in Section 15.5 *Security Assessment and Authorization Requirements* for review and approval by the GAC Project Authority, prior to commencing the next phase of development.

15.5 Security Assessment and Authorization Requirements

The requirements for each SA&A phase are described below.

[14] https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33

15.5.1 Security Assessment and Authorization Phase-1 Requirements (High-Level Security Design)

The **Phase-1 Review Point** is established after completion of the following:

15.5.1.1 The Contractor must provide a High-Level Security Design that must include:

a) a high-level component diagram that clearly shows the overall architecture, the allocation of services and components to network security zones, and identifies key security-related data flows;
b) a description of the network zone perimeter defenses;
c) a description of the approach to data segregation;
d) descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;
e) descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;
f) allocation of the security requirements at each of the architecture layers of the high-level service design;
g) definition of the architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer);
h) a description of the approach for remote management;
i) a description of the approach for access control;
j) a description of the approach for security management and audit;
k) a description of the approach for configuration management;
l) a description of the approach for patch management;
m) a description of the approach for the disposal and sanitization of Canada's data;
n) the decommissioning process to follow when the system is no longer required; and
o) justification for key design decisions.

15.5.1.2 The Contractor must provide a Security Requirements Traceability Matrix (SRTM) that contains the following information for each security requirement in the **TBS Playbook for SaaS Applications Up to PROTECTED B** SRTM, IB# **14310732**:

a) the security requirement identifier (SR);
b) the security requirement statement;
c) a description of how the security requirement is addressed in the High-Level Security Design in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements; and
d) the title of the Contract deliverable(s) in which the Contractor will provide the details of its security solution for the requirement (e.g., Service Continuity Plan)

15.5.2 Security Assessment and Authorization Phase-2 Requirements (Detailed Security Design)

The **Phase-2 Review Point** is established after completion of the following:

15.5.2.1 The Contractor must provide a Detailed Security Design that includes:

a) a detailed component diagram (this must be a refinement of the high-level component diagram);
b) descriptions of the allocation of technical security mechanisms to detailed service design elements;
c) descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and
d) justification for key design decisions.

15.5.2.2 The Contractor must provide a Security Requirements Traceability Matrix (SRTM) that contains the following information for each security requirement in the **TBS Playbook for SaaS Applications Up to PROTECTED B** SRTM, IB# **14310732**:

a) the security requirement identifier (SR);
b) the security requirement statement;
c) a description of how the security requirement is addressed in the Detailed Security Design in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements; and
d) the title of the Contract deliverable(s) in which the Contractor will provide the details of its security solution for the requirement (e.g., Service Continuity Plan)

15.5.3 Security Assessment and Authorization Phase-3 Requirements (Implementation)

The **Phase-3 Review Point** is established after completion of the following:

15.5.3.1 The Contractor must provide a Security Test Plan that includes:

a) the security functions to be tested; and
b) for each security function or sets of security functions, the items to be tested including:
    (i) a description of the test case, procedure, or scenario;
    (ii) environmental requirements;
    (iii) ordering dependencies; and
    (iv) expected results (i.e., pass/fail criteria).

15.5.3.2 The Contractor must provide Canada with an updated SRTM that contains, for each security requirement to be tested by the Security Test Plan, the tracing (a reference to an identifiable element) to security testing test cases.

15.5.3.3 The Contractor must provide a Vulnerability Assessment (VA) Plan that includes:

a) a description of the scope of the vulnerability assessment;
b) a description of the vulnerability assessment process; and
c) a description of the vulnerability assessment tools that will be used, including any software versions.

15.5.3.4 The Contractor must provide a Security Installation Verification Plan that includes:

a) the security verification approach;
b) an outline of the security verification items; and
c) for each security verification item:
    (i) a description of the verification scenario;
    (ii) ordering dependencies; and
    (iii) expected results (i.e. pass/fail criteria).

15.5.3.5 The Contractor must conduct security installation verification in accordance with the Security Installation Verification Plan.

15.5.3.6 The Contractor must provide Canada with an updated SRTM that contains, for each security requirement to be tested by the Security Installation Verification Plan, the tracing (a reference to an identifiable element) to security installation verification test cases.

15.5.3.7 The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

15.5.3.8 The Security Installation Verification Report must include for each of the test items in the security installation verification plan:

a) the expected results;
b) the actual results; and
c) a description of deviations and how each was resolved.

15.5.3.9 The Contractor must conduct security testing in accordance with the Security Test Plan.

15.5.3.10 The Security Test Report must include, for each of the test items in the Security Test Plan:

a) the expected results (i.e. pass/fail criteria);
b) the actual results; and
c) a description of deviations and how each was resolved.

15.5.3.11 The Contractor must conduct vulnerability assessments in accordance with the Vulnerability Assessment Plan and produce a Vulnerability Assessment Report.

15.5.3.12 The Vulnerability Assessment Report must include:

a) a listing of the vulnerability assessment results;
b) for each vulnerability detected:
    (i) an assessment of the severity of the vulnerability (e.g. Common Vulnerability Scoring System (CVSS)[15]); and

[15] https://www.first.org/cvss/

(ii) a description of the patch or corrective measure that was implemented to resolve the vulnerability.

c) for any unresolved vulnerability:

(i) an assessment of the significance of the vulnerability; and

(ii) the rationale for not implementing a patch or a corrective measure.

15.5.3.13 The Contractor must implement patches and corrective measures as part of vulnerability assessment activity.

ANNEX E, ELECTRONIC PAYMENT INSTRUMENTS

The Contractor accepts to be paid using 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)

ATTACHMENT 4.1, BID EVALUATION CRITERIA

1.1 TECHNICAL CRITERIA

a) It is recommended that the Bidder include a grid in their proposals, cross-referencing statements of compliance with the supporting data in their proposals. Note: the compliance grid, by and of itself does not constitute demonstrated evidence. The Bidder must submit a detailed CV for each of the proposed resources.

b) Education must have been obtained from a recognized* Canadian university, college or high school, or the equivalent as established by a recognized* Canadian academic credentials assessment service, if obtained outside Canada.

*The list of recognized Canadian academic credentials assessment service providers can be found under the Canadian Information Centre for International Credentials website, at the following Internet link: http://www.cicic.ca/indexe.stm.
In order to obtain points for education and professional accreditations, the Bidder should also include photocopies of certificates. If not provided with the bid, Bidders must provide them upon request and in the timeframe stated by the Contracting Authority.

c) The Bidder is advised that only listing experience without providing any supporting data to describe where and how such experience was obtained will not constitute “demonstrated” for the purpose of the evaluation.

Each project summary should include the name, phone number or e-mail of client reference. Canada reserves the right to request and contact Client references to validate information in the proposal.

The Bidder should provide complete details as to where, when (month and year) and how (through which activities/responsibilities) the stated qualifications/experience were obtained. Experience gained during formal education should not be considered work experience. All requirements for work experience should be obtained in a legitimate work environment as opposed to an educational setting. Co-op terms are considered work experience as they are related to the required services.

Bidders are also advised that the month(s) of experience listed for a project whose timeframe overlaps that of another referenced project will only be counted once. For example: Project 1 timeframe is July 2001 to December 2001; Project 2 timeframe is October 2001 to January 2002; the total months of experience for these two projects references is seven (7) months. Bidders are asked to indicate on the resumes how many months/years are to be counted for each project.

For each criterion, details should be provided regarding the qualifications, relevant experience and expertise of the proposed personnel. For mandatory and point rated requirements, the experience of the proposed resource(s) must be clearly identified by providing a summary/description of the previous projects worked on and indicating when the work was carried out, and the client. The evaluation criteria matrix must be used to answer the mandatory and point rated criteria. Therefore, the answers are to be entered directly into the matrix, explaining how each criterion has been met, while referencing both the page and project numbers as indicated in the resume.

d) It is recommended that the Bidder also include in the CV, the current level of personnel security held by the proposed resource and their corresponding Canadian Industrial Security Directorate (CISD) file number.

e) Reference Checks and Interviews may be sought: If reference checks are conducted by Canada, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day. Canada will not award any points unless the response is received within 5 working days. Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated. Points will not be allocated if the reference customer is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder). Nor will points be allocated if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder. Crown references will be accepted.

The project and contract summaries cited must include the following information:

- Name of the client organization;
- Contract start and end dates (DD/MM/YYYY to DD/MM/YYYY);
- The dollar value of the project ($CAD);
- Brief description of the services provided (including roles and activities performed by the proposed resource); and
    - Client Reference information should include: name, title and telephone number and email address of the client's project or technical authority.

Unless otherwise stated, projects must be a minimum duration of four (4) months to be considered.

Definitions:

- **Stakeholder**: A Stakeholder is an individual or organization that has/had influence over a project's objectives and outcomes, is/was involved in the project delivery or project oversight, and whose interests may be affected as a result of project execution or project completion.

- **Federal Government Organization or Agency**: A Federal Government Organization or Agency is defined as an organization listed in Schedule I, II, III, V or VI (Part 1) of the Financial Administration Act). Website: http://laws-lois.justice.gc.ca/eng/acts/F-11/index.html

- **Senior Executive Management**: Senior Executive Management is defined as Chief Executive Officer (CEO), Chief Information Officer (CIO), Associate Deputy Minister (ADM), Vice President (VP), Chief Operations Officer (COO), and Chief Financial Officer (CFO). In the private sector, Senior Executive Management is defined as President, Vice President (VP), Chief Operating Officer and Chief Executive Officer (CEO).

- **National**: National is defined as impacting operations in a minimum of four (4) provinces/territories.

- **Large Project**: A Large Project is defined as a project or program that must meet the following characteristics:

- Scope spans multiple programs/services involving at least one external Federal government organization or Agency or private enterprise.
- Has a project duration of over 12 months.
- Has a peak project team size of over 45 people (employees and contractors).
- Supports an organization of over 1000 employees.

- **Public Sector** shall include Federal (including Crown Corporations), Provincial and Municipal government organizations as well as any quasi-governmental organization in Canada.
- ** Large Public Organizations shall be defined as follows: All government organizations, including the Federal, provincial, municipal levels of government. Public-sector organizations that focus on services to the public as a whole, including education, welfare, the legal system and health care services.

1.2 Mandatory Criteria

The bid must meet the mandatory technical criteria specified below. Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below. The Bidder must provide the necessary documentation to support compliance with this requirement.

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

ITEM	MANDATORY CRITERIA	MET / NOT MET	CROSS REFERENCE TO PROPOSAL
Operational Requirements			
M1	Bidder must propose a SaaS omnichannel communications platform that will permit Canadian citizens in distress overseas to communicate with the EWRC using modern communications channels and demonstrate that the platform: -Incorporates, at a minimum, the following communication channels: SMS, WhatsApp, live chat. -Is able to onboard and offboard new channels in response to shifting usage patterns of social media and chat applications. -Platform must allow for 30 concurrent logins.		
M2	Bidder must demonstrate that their platform: -Incorporates all communications into a single engagement hub.		

	-Incorporates workflow automation tools, such as pre-approved response messages, automated response messages, message routing, etc. -Has the ability to export conversation data		
M3	Bidder must confirm that their platform: -Can be delivered through a software-as-a-service model. -Supports multiple languages, including English and French -Allows for third-party integration capability with Microsoft Dynamics 365. -Has flexible data retention and disposal framework that can be aligned with GAC's requirements. -Operates with high-level availability and with data centre level redundancy. -Processes and stores all data in Canada -Provides 24/7 technical support for contact centre agents.		
M4	Bidder must demonstrate that their platform: -Meets technical security standards, including: -ISO/IEC 27001:2013 (also known as ISO 27001); and -AICPA SOC 2 Type II in accordance with Annex D, IT Security Requirements Technical Annex -Provides account management and detailed audit functionalities.		
M5	Project authority must provide details on the project implementation plan, including names and bios of implementation team members, and outline of the implementation plan,		

Note: The successful Bidder undertakes to work with GAC Information Technology security personal to complete an internal Security Assessment and Authorization process set out in Annex D IT Security Technical Annex and in particular, to complete the documents identified in Section 14.

2.0 Point Rated Criteria

Proposals will be evaluated and scored in accordance with specific evaluation criteria as detailed in this section.

ITEM	POINT-RATED REQUIREMENT	MAX Score	POINT ALLOCATION	BIDDER'S RESPONSE & DEMONSTRATED EXPERIENCE
Platform Capability				
R1	Concurrently communicate, with multiple clients using multiple communications channels. The user interface should be simple and intuitive, and create an operating environment for agents that enable effective and efficient workflows.	10	Demonstrates that the Bidders web-based platform has the required capability. Information is clear and detailed. Examples of previous projects have been provided. 10 points. Demonstrates that the Bidder's web-based platform has the required capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R2	Utilize ChatBot technology that can be applied to all integrated communications channels globally or as per routing rules and that uses Natural Language Processing (NLP) to ensure contextual understanding. ChatBot must function in both English and French.	10	Demonstrates that the Bidders web-based platform has the required capability. Information is clear and detailed. Examples of previous projects have been provided. 10 points. Demonstrates that the Bidder's web-based platform has the required capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R3	Deliver a variety of data analytics tools and pre-	10	Demonstrates that the Bidders web-based platform has the required capability. Information is clear and	

	configured custom reporting tools.		detailed. Examples of previous projects have been provided. 10 points. Demonstrates that the Bidder's web-based platform has the required capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R4	Configure the live chat interface for integration into Global Affairs Canada websites; Bidder must demonstrate the English and French client-side interface of live chat.	10	Demonstrates that the Bidders web-based platform has the required capability. Information is clear and detailed. Examples of previous projects have been provided. 10 points. Demonstrates that the Bidder's web-based platform has the required capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
Minimum Pass Mark: 30			**Score:**	

ITEM	**POINT-RATED REQUIREMENT**	**MAX Score**	**POINT ALLOCATION**	**BIDDER'S RESPONSE & DEMONSTRATED EXPERIENCE**
Training and Technical Support: The Bidder should demonstrate their methods and level of experience with respect to their omnichannel communications platform, within the last three (3) years from the closing date of this RFP, in providing:				

R5	Distance and/or in-person training to individuals in small groups	10	Demonstrates the Bidder has the required in-house capability. Information is clear and detailed. Demonstrates a minimum of 2 years' experience in the last three years. 10 points. Demonstrates the Bidder has the required in-house capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R6	Support to help agents experiencing difficulties navigating the platform	10	Demonstrates the Bidder has the required in-house capability. Information is clear and detailed. Demonstrates a minimum of 2 years' experience in the last three years. 10 points. Demonstrates the Bidder has the required in-house capability but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R7	Training methods as per the Statement of Work	10	Training methods addressed and demonstrates that the Bidder has the capability to provide the training required as outlined in the Statement of Work and is further supported by in-person online training tools	

			and technical support availability during business hours. 10 points. Training methods addressed and demonstrates that the Bidder has the capability to provide the training required as outlined in the Statement of Work but has one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	
R8	Technical Support as per the Statement of Work	10	Technical support addressed and demonstrates that the Bidder has the capability to provide telephone access to their technical support staff 7 days a week/24 hours a day. 10 points. Technical support addressed and demonstrates that the Bidder has the capability to provide telephone access to their technical support staff during business hours as identified in the statement of work and/or there is one unclear element. 7 points. The Bidder's proposed platform does not have the required capability and/or there are more than one unclear element in the submission. 0 points.	

Minimum Pass Mark: 30	Score:

Demonstration

Prior to contract award, Bidders may be requested to provide a live demonstration to demonstrate that their system is able to meet all the requirements as described in the Statement of Work and to validate operational requirements. Canada reserves the right to declare a bid non-responsive, in the event that the Bid Evaluation Team determines that the Bidder has not successfully demonstrated their technical ability the meet the requirement as requested.

The demonstration must be conducted virtually and at no cost to Canada. It must not exceed 1 hour in length.

Canada will provide no fewer than five days working days of notice before the scheduled date for the demonstration.