Royal Canadian Mounted Police / Gendarmerie royale du Canada

**RETURN BIDS TO:**
**RETOURNER LES SOUMISSIONS À** :

Bid Receiving/Réception des soumissions

**angelo.kaldis@rcmp-grc.gc.ca**

# REQUEST FOR PROPOSAL

# DEMANDE DE PROPOSITION

Proposal to: Royal Canadian Mounted Police

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 hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux : Gendarmerie royale du Canada

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

| **Title – Sujet**<br>**Annual Flight and Crew Member Mandatory Web-Based Training** | | **Date**<br>**2023/04/24** |
|---|---|---|
| **Solicitation No. – Nº de l'invitation**<br>**202105319** | | |
| **Client Reference No. - No. De Référence du Client**<br>**202105319** | | |
| **Solicitation Closes – L'invitation prend fin** | | |
| **At /à :** | **14 :00** | EDT (Eastern Daylight Time)<br>HAE (heure avancée de l'Est) |
| **On / le :** | **2023/06/13** | |

| **Delivery - Livraison**<br>See herein — Voir aux présentes | **Taxes - Taxes**<br>See herein — Voir aux présentes | **Duty – Droits**<br>See herein — Voir aux présentes |
|---|---|---|

**Destination of Goods and Services – Destinations des biens et services**
See herein — Voir aux présentes

**Instructions**
See herein — Voir aux présentes

**Address Inquiries to –**
**Adresser toute demande de renseignements à**
**Angelo Kaldis**
**Procurement Specialist, HQ Procurement and Contracting**
**angelo.kaldis@rcmp-grc.gc.ca**

**Telephone No. – No. de téléphone**
**519-318-3897**

| **Delivery Required** –<br>**Livraison exigée**<br>See herein — Voir aux présentes | **Delivery Offered** –<br>**Livraison proposée** |
|---|---|
| **Vendor/Firm Name, Address and Representative – Raison sociale, adresse et représentant du fournisseur/de l'entrepreneur :** | |
| **Telephone No. – No. de téléphone** | **Facsimile 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** |

Canada

## TABLE OF CONTENTS

**List of Annexes:**

## 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 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 Check List (SRCL) & Security Guide and the Evaluation Criteria.

### 1.2 Summary

**1.2.1** The Royal Canadian Mounted Police (RCMP) has a requirement for annual web-based aviation specific training. Training is to ensure that approximately 165 RCMP Air Services personnel inclusive of Pilots, Aircraft Maintenance Engineers (AME), Tactical Flight Officers and Flight Coordinators meet Transport Canada and RCMP requirements to maintain a safe competency level. RCMP Air Services is authorized to operate aircraft as a Private Operator provided its Fixed and Rotary Pilots, AMEs and Crew Members complete mandatory training topics, many of which can be administered through a web-based solution, that meet or exceed Canadian Aviation Regulations (CARs). The Contractor must perform the work in accordance with Annex "A" – Statement of Work.

Any resulting contract (1 contract only), will be valid from date of contract award for one (1) year, with the irrevocable option to extend the term of the contract by up to four (4) additional one (1) year periods under the same terms and conditions.

The requirement is subject to the provisions of the Canadian Free Trade Agreement (CFTA), Canada Chile Free Trade Agreement, Canada Columbia Free Trade Agreement, Canada Honduras Free Trade Agreement, Canadas Panama Free Trade Agreement, Canada Panama Free Trade Agreement, Canada Peru Free Trade Agreement and Canada Ukraine Free Trade Agreement.

**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. Please note, the above website is specific to PWGSC requirements and processes may differ from RCMP requirements.

## 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.

## 1.4 Recourse Mechanisms

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

https://buyandsell.gc.ca/for-businesses/selling-to-the-government-of-canada/bid-follow-up/bid-challenge-and-recourse-mechanisms

http://opo-boa.gc.ca/plaintesurvol-complaintoverview-eng.html

## 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.

Revision to Departmental Name: As this solicitation is issued by Royal Canadian Mounted Police (RCMP), any reference to Public Works and Government Services Canada or PWGSC or its Minister contained in any term, condition or clause of this solicitation, including any individual SACC clauses incorporated by reference, will be interpreted as reference to RCMP or its Minister.

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: 180 days

### 2.2 Submission of Bids

Bids must be submitted only to RCMP Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation.

NOTE: The RCMP has not been approved for bid submission by Canada Post Corporation (CPC) Connect service.

Bids transmitted by facsimile to RCMP will not be accepted.

### 2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than seven (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.

## 2.4 Applicable Laws

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

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

## 2.5 Promotion of Direct Deposit Initiative

The following information is not related to the solicitation process:

An initiative within the Government of Canada called the Cheque Standardization Project has been established whereby eventually for all payments, cheque stubs will no longer be printed and, with few exceptions, will be processed via direct deposit. This option is only available when payment is made in Canadian dollars for deposit into a Canadian bank account. In an attempt to be proactive, RCMP Corporate Accounting is promoting the registration of RCMP suppliers for the upcoming change in the payment process.

If you are the successful Bidder on this or any other RCMP requirement, you are encouraged to register with the RCMP for direct deposit. Please contact RCMP Corporate Accounting by email to receive a form entitled *Recipient Electronic Payment Registration Request* along with instructions for completion of the form.

Should you have any questions regarding the Cheque Standardization Project or if you want to register, please contact the following email: corporate_accounting@rcmp-grc.gc.ca

## 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 seven (7) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

## 2.7 Volumetric Data

The volumetric data of the estimated number of learners has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of the service identified in this bid solicitation will be consistent with this data. It is provided purely for information purposes.

## PART 3 - BID PREPARATION INSTRUCTIONS

### 3.1 Bid Preparation Instructions

Canada requests that the Bidder submit their complete email bid in separately saved and attached sections as follows:

**Section I: Technical Bid** (one soft copy in PDF format)

**Section II: Financial Bid** (one soft copy in PDF format)

**Section III: Certifications** (one soft copy in PDF format)

**Important Note:**

For bids transmitted by email, Canada will not be responsible for any failure attributable to the transmission or receipt of the bid including, but not limited to, the following:

a) receipt of garbled or incomplete bid;

b) delay in transmission or receipt of the bid to the Contracting Authority's email inbox (the date & time on the email received by the Contracting Authority is considered the date & time of receipt of the bid submission);

c) availability or condition of the receiving equipment;

d) incompatibility between the sending and receiving equipment;

e) failure of the Bidder to properly identify the bid;

f) illegibility of the bid; or

g) security of bid data.

A bid transmitted electronically constitutes the formal bid of the Bidder and must be submitted in accordance with Section 05 of 2003 (2022-03-29) Standard Instructions - Goods or Services - Competitive Requirements.

The RCMP has restrictions on incoming e-mail messages. The maximum e-mail message size including all file attachments must not exceed 5MB. Zip files or links to bid documents will not be accepted. Incoming e-mail messages exceeding the maximum file size and/or containing zip file attachments will be blocked from entering the RCMP e-mail system. A bid transmitted by e-mail that gets blocked by the RCMP e-mail system will be considered not received. It is the responsibility of the Bidder to ensure receipt.

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

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

a) use a numbering system that corresponds to the bid solicitation.

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, duotangs 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 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 Exchange Rate Fluctuation**

C3011T (2013-11-06) Exchange Rate Fluctuation

**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" and "financial" 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 Annex D.

#### 4.1.2 Financial Evaluation

##### 4.1.2.1 Mandatory Financial Criteria

*SACC Manual* Clause A0220T (2014-06-26) Evaluation of Price-Bid

### 4.2 Basis of Selection - Highest Combined Rating of Technical Merit and Price

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
2. Bids not meeting a) or b) 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 20% for the technical merit and 80% 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 20%.
5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 80%.
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 20/80 ratio of technical merit and price, respectively. The total available points equals 20 and the lowest evaluated price is $45,000 (45).

**Basis of Selection - Highest Combined Rating Technical Merit (20%) and Price (80%)**

| | | Bidder 1 | Bidder 2 | Bidder 3 |
|---|---|---|---|---|
| **Overall Technical Score** | | 10/20 | 20/20 | 10/20 |
| **Bid Evaluated Price** | | $55,000.00 | $50,000.00 | $45,000.00 |
| **Calculations** | **Technical Merit Score** | 10/20 x 20 =10 | 20/20 x 20 = 20 | 10/20 x 20 = 10 |
| | **Pricing Score** | 45/55 x 80 = 65.45 | 45/50 x 80 = 72.00 | 45/45 x 80 = 80.00 |
| **Combined Rating** | | 75.45 | 92.00 | 90 |
| **Overall Rating** | | 3rd | 1st | 2nd |

## PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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

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

#### 5.1.1 Integrity Provisions

In accordance with the section titled Information to be provided when bidding, contracting, or entering into a real property agreement subject to 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:

- Declaration of Convicted Offences - Integrity Declaration Form (as applicable)
- Required Documentation (List of names for integrity verification form)

Please see the Forms for the Integrity Regime website for further details (http://www.tpsgc-pwgsc.gc.ca/ci-if/formulaires-forms-eng.html).

#### 5.1.2 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 (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#).

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.

### 5.1.3 Additional Certifications Precedent to Contract Award

#### 5.1.3.1 Independent Bid Determination

The attached Certificate of Independent Bid Determination (attached ATTACHMENT 1 to PART 5 - CERTIFICATE OF INDEPENDENT BID DETERMINATION) has been developed by the federal Competition Bureau for use by the Contacting Authority when calling for bids, tenders or quotations. The intention of this documentation is to deter bid-rigging by requiring Bidders to disclose, to the Contracting Authority, all material facts about any communications and arrangements which the Bidder has entered into with competitors regarding the call for tenders.

#### 5.1.3.2 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.

#### 5.1.3.3 Software as a Service (SaaS) Publisher Certificate Form

If the SaaS Publisher (defined as the entity or person who is the owner of the copyright in any SaaS Solution included in the Submission and who has the right to the license and to authorize others to use its SaaS Solution and any underlying components) intends to submit a Submission and qualify itself as a Supplier, such SaaS Publishers must submit the certification at Attachment 2 to Part 5.

## ATTACHMENT 1 to PART 5 - CERTIFICATE OF INDEPENDENT BID DETERMINATION

I, the undersigned, in submitting the accompanying bid or tender (hereinafter "bid") to:

_____
(Corporate Name of Recipient of this Submission)

for: _____
(Name and Number of Bid and Project)

in response to the call or request (hereinafter "call") for bids made by:

_____
(Name of Tendering Authority)

do hereby make the following statements that I certify to be true and complete in every respect:

I certify, on behalf of: _____ that:
(Corporate Name of Bidder or Tenderer [hereinafter "Bidder"])

1. I have read and I understand the contents of this Certificate;

2. I understand that the accompanying bid will be disqualified if this Certificate is found not to be true and complete in every respect;

3. I am authorized by the Bidder to sign this Certificate, and to submit the accompanying bid, on behalf of the Bidder;

4. each person whose signature appears on the accompanying bid has been authorized by the Bidder to determine the terms of, and to sign, the bid, on behalf of the Bidder;

5. for the purposes of this Certificate and the accompanying bid, I understand that the word "competitor" shall include any individual or organization, other than the Bidder, whether or not affiliated with the Bidder, who:
   (a) has been requested to submit a bid in response to this call for bids;
   (b) could potentially submit a bid in response to this call for bids, based on their qualifications, abilities or experience;

6. the Bidder discloses that (check one of the following, as applicable):
   (a) the Bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with, any competitor;

   (b) the Bidder has entered into consultations, communications, agreements or arrangements with one or more competitors regarding this call for bids, and the Bidder discloses, in the attached document(s), complete details thereof, including the names of the competitors and the nature of, and reasons for, such consultations, communications, agreements or arrangements;

7. in particular, without limiting the generality of paragraphs (6)(a) or (6)(b) above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
   (a) prices;
   (b) methods, factors or formulas used to calculate prices;
   (c) the intention or decision to submit, or not to submit, a bid; or
   (d) the submission of a bid which does not meet the specifications of the call for bids;
   except as specifically disclosed pursuant to paragraph (6)(b) above;

8. in addition, there has been no consultation, communication, agreement or arrangement with any competitor regarding the quality, quantity, specifications or delivery particulars of the products or services to which this call for bids relates, except as specifically authorized by the Tendering Authority or as specifically disclosed pursuant to paragraph (6)(b) above;

9. the terms of the accompanying bid have not been, and will not be, knowingly disclosed by the Bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening, or of the awarding of the contract, whichever comes first, unless otherwise required by law or as specifically disclosed pursuant to paragraph (6)(b) above.

_____

(Printed Name and Signature of Authorized Agent of Bidder)

_____ _____

(Position Title) (Date)

**ATTACHMENT 2 to PART 5 - SaaS Publisher Certification Form**

**Form 1 – SaaS Publisher Certification Form**

*(to be used where the Contractor itself is the SaaS Publisher)*

The Contractor certifies that they are the Software as a Service (SaaS) Publisher of all the following SaaS Solutions and that it has all the rights necessary to license them in accordance with the terms and conditions of the contract to Canada:

_____

_____

_____

_____

_____

*(Contractor should add or remove lines as needed, or attach the product list as an appendix)*

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher _____

Print Name of authorized signatory of SaaS Publisher _____

Print Title of authorized signatory of SaaS Publisher _____

Address for authorized signatory of SaaS Publisher _____

Telephone no. for authorized signatory of SaaS Publisher _____

Email for authorized signatory of SaaS Publisher _____

Date signed _____

## PART 6 - SECURITY REQUIREMENTS

### 6.1 Security Requirements

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

   a) the Bidder's proposed Cloud Services must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

   b) the Bidder is required to participate in any Security Assessment and Authorization (SA&A) process deemed necessary by the Project Authority and/or Departmental Security (DS). Before any solutions developed in whole or in part by bidders are moved into a production environment a full Authority to Operate (ATO) must be granted. Obtaining an ATO requires a security assessment as part of the Security Assessment and Authorization (SA&A) process, which can be initiated by contacting Departmental Security (DS). Refence section 6.3 IT Security Assessment and Authorization Process in the Security Guide in Annex C.

2. Bidders are reminded to obtain the required security authorization 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.

## 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".

### 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.

Revision to Departmental Name: As this contract is issued by Royal Canadian Mounted Police (RCMP), any reference to Public Works and Government Services Canada or PWGSC or its Minister contained in any term, condition or clause of this contract, including any individual SACC clauses incorporated by reference, will be interpreted as reference to RCMP or its Minister.

#### 7.2.1 General Conditions

2035 (2022-12-01) General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

### 7.3 Security Requirements

**7.3.1** The following security requirements (Annex C – Security Requirements Check List (SRCL) & Security Guide) apply and form part of the Contract.

#### 7.3.2 IT Security Assessment and Authorization Process

**7.3.2.1** The Bidder must ensure through the RCMP Information and Communications Technology Security (ICTS) that the Bidder holds a valid Authority to Operate (ATO).

## 7.4 Term of Contract

### 7.4.1 Period of the Contract

The period of the Contract is from date of Contract to _____ inclusive **(dates to be inserted at contract award).**

### 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 four (4) additional one (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 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: Angelo Kaldis
Title: Procurement Specialist, HQ Procurement and Contracting
Royal Canadian Mounted Police
Telephone: 519-318-3897
E-mail address: angelo.kaldis@rcmp-grc.gc.ca

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 (to be identified at contract award)

The Project Authority for the Contract is:

Name: _____
Title: _____
Royal Canadian Mounted Police
Directorate: _____
Address: _____

Telephone: ___-___-_____
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 identified at contract award)

The Contractor's Representative for the Contract is:

Name: _____
Title: _____
Address: _____

Telephone: ___-___-_____
E-mail address: _____

## 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 – Firm Unit Prices

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm unit prices, as specified in Annex "B" for a cost of $ _____ **(to be inserted at contract award).** Customs duties are included and Applicable Taxes are extra.

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

### 7.7.2 Limitation of Expenditure

1. Canada's total liability to the Contractor under the Contract must not exceed $ _____ **(to be inserted at contract award)**. 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 – Multiple Payments

*SACC Manual* clause H1001C (2008-05-12) Multiple Payments

### 7.7.4 Taxes - Foreign-based Contractor

*SACC Manual* clause C2000C (2007-11-30) Taxes - Foreign-based Contractor

## 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. Invoices must be distributed as follows:
   a) One (1) copy must be forwarded to the Project Authority identified under the section entitled "Authorities" of the Contract for certification and payment.
   b) 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 _____ **(to be inserted at contract award).**

## 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 general conditions 2035 (2022-12-01) General Conditions - Higher Complexity - Services;
c) Annex A, Statement of Work;
d) Annex B, Basis of Payment;
e) Annex C, Security Requirements Check List;
f) the Contractor's bid dated _____ **(to be inserted at contract award).**

## 7.12 Procurement Ombudsman

### 7.12.1 Dispute Resolution

The Parties agree to make every reasonable effort, in good faith, to settle amicably all disputes or claims relating to the Contract, through negotiations between the Parties' representatives authorized to settle. If the Parties do not reach a settlement within 25 working days after the dispute was initially raised to the other party in writing, either Party may contact the Office of the Procurement Ombudsman (OPO) to request dispute resolution/mediation services. OPO may be contacted by e-mail at boa.opo@boa-opo.gc.ca, by telephone at 1-866-734-5169, or by web at www.opo-boa.gc.ca. For more information on OPO's services, please see the Procurement Ombudsman Regulations or visit the OPO website.

### 7.12.2 Contract Administration

The parties understand that the Procurement Ombudsman appointed pursuant to Subsection 22.1(1) of the *Department of Public Works and Government Services Act* will review a complaint filed by the complainant respecting administration of this contract if the requirements of Subsection 22.2(1) of the *Department of Public Works and Government Services Act* and Sections 15 and 16 of the *Procurement Ombudsman Regulations* have been met.

To file a complaint, the Office of the Procurement Ombudsman may be contacted by e-mail at boa.opo@boa-opo.gc.ca, by telephone at 1-866-734-5169, or by web at www.opo-boa.gc.ca.

## 7.13 Insurance

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

# ANNEX A - STATEMENT OF WORK

## 1. TITLE

RCMP Annual Flight and Crew Member Mandatory Web-based Training

## 2. BACKGROUND

Annual aviation specific training is a Transport Canada requirement to ensure pilots, aircraft maintenance engineers and crew members (Tactical Flight Officers/Flight Coordinators) maintain a safe competency level. These requirements are found in the Canadian Aviation Regulations (CARS) Part VI, subpart 4. Under these regulations, RCMP Air Services is authorized to operate aircraft as a Private Operator provided its pilots and aircraft maintenance engineers complete mandatory training topics, many of which can be administered through a web-based solution. This statement of work is in accordance with the RCMP Fixed Wing Operations Manual (FWOM), the RCMP Rotary Wing Operations Manual (RWOM), sections 6: Training and Proficiency Requirements, and the RCMP Maintenance Control Manual (MCM). These manuals ensure compliance with CARS 604 training requirements.

## 3. ACRONYMS

| | |
|---|---|
| ACAS | Airborne Collision Avoidance System |
| AME | Aircraft Maintenance Engineer |
| CARS | Canadian Aviation Regulations |
| CFIT | Controlled flight into terrain |
| FW | Fixed Wing (Airplane) |
| FWOM | Fixed Wing Operations Manual |
| MCM | Maintenance Control Manual |
| NASA | National Aeronautics and Space Administration |
| RCMP | Royal Canadian Mounted Police |
| RW | Rotary Wing (Helicopter) |
| RWOM | Rotary Wing Operations Manual |
| SOW | Statement of Work |
| TA | Technical Authority |
| TCAS | Traffic Collision Avoidance System |
| TFO | Tactical Flight Operations |
| WHMIS | Workplace Hazardous Materials Information System |

## 4. APPLICABLE DOCUMENTS & REFERENCES

1. RCMP Fixed Wing Operations Manual
   - Section 6.6 Training Programs
2. RCMP Rotary Wing Operations Manual
   - Section 6.6 Training Program
3. RCMP Maintenance Control Manual
   - Section 4.1.1
4. Canadian Aviation Regulations
   - Section 604 Private Operators

## 5. TASKS

The Contractor must provide web-based self-paced training on the following aviation topics. The topics are learner group specific and the Contractor must ensure that each topic contains relevant Canadian aviation content. The topics listed below are the minimum required.

### 5.1 Fixed Wing Pilots (max. 50 learners):

a) ACAS/TCAS
b) Airborne Icing
c) Aircraft Critical Surface Contamination
d) Canadian – US Differences
e) CFIT- Controlled Flight into Ground
f) Crew Resource Management
g) Emergency Procedures Training
h) Fatigue Management
i) High Altitude and Physiology and Effects
j) Human Factors for pilots
k) Meteorology review
l) No Carry Transportation of Dangerous Goods
m) Operations Review – 604 specific
n) Performance Airspace
o) Radar review
p) Reduced Vertical Separation Minimum
q) Runway Incursion Awareness
r) Safety Management Systems
s) Single Pilot Resource Management
t) Survival Principles
u) Threat and Error Management
v) Towing Aircraft

**5.2 Rotary Wing Pilots (max. 20 learners):**

a) Airborne Icing
b) Aircraft Critical Surface Contamination
c) CFIT- Controlled Flight into Ground
d) Crew Resource Management
e) Emergency Procedures Training
f) Fatigue Management
g) High Altitude and Physiology and Effects
h) Human Factors for pilots
i) Meteorology review
j) No Carry Transportation of Dangerous Goods
k) Operations Review – 604 specific
l) Runway Incursion Awareness
m) Safety Management Systems
n) Single Pilot Resource Management
o) Survival Principles
p) Threat and Error Management
q) Towing Aircraft

**5.3 Aircraft Maintenance Engineers (max. 45 learners):**

a) Emergency Procedures Training
b) Fatigue Management
c) Maintenance Resource Management
d) Human Factors for Engineers
e) Maintenance review – Operations, Regulations and Standards
f) No Carry Transportation of Dangerous Goods
g) RVSM for Maintenance
h) Runway Incursion Awareness
i) Towing aircraft

**5.4 Crew Members (Tactical Flight Officers and Flight Coordinators) (max. 50 learners):**

a) Airborne Icing
b) Aircraft Critical Surface Contamination
c) Controlled flight into terrain (CFIT)
d) Crew Resource management
e) Emergency Procedures Training
f) High Altitude Physiology and Effects
g) No carry dangerous goods awareness

**5.5 Occupational Health and Safety topics available to all learner groups.**

a) Back injury prevention
b) Communicable Disease Prevention
c) Confined Space Awareness
d) Electrical Safety
e) Ergonomics
f) Fall Protection
g) Fire Prevention
h) Fuel and Ignition awareness
i) Personal Protective Equipment
j) WHMIS

**5.6 Administrative Tasks**

The Contractor must complete the following administrative tasks in addition to providing the required web-based self-paced training:

a) Maintain web-based audit ready records of training for learners.
b) Via web link, provide 10 RCMP Air Service administrators access to the web-based training records of RCMP employees. Administrators at a minimum must be able to view the following individual's training information:
    i. name
    ii. list of assigned topics
    iii. date the topic was completed
    iv. date the topic expires
c) Administrator roles must be distinct from learner roles as administrators can also be learners.
d) Utilize subject matter experts to keep training topics current. Examples of subject matter experts include: Flight Safety Foundation for Controlled Flight into Terrain and NASA/Canadian National Research Council for Icing.
e) A web-based exam must be provided for each module found within each training topic
f) Email an annual report on the topics provided to ensure the RCMP's compliance with Canadian Aviation Regulations 604 (CARS 604).
g) Generate email notifications to learners and administrators:
    i. Assigning a topic when it is available for the learner to access.
    ii. Within two (2) weeks of when an individual's training topic is overdue. Overdue is defined as not being completed within 2 weeks of being assigned.

**5.7 Technical Requirements**

a) The Training solution must be compatible with the following internet browsers:
   i. Microsoft Edge v. 106 and subsequent versions;
   ii. Google Chrome v.106 and subsequent versions;
   iii. Safari on iOS 9.3 and higher

b) The Training Solution must have the ability to associate Canada unique identifiers (e.g. RCMP email address, etc.) with the corresponding cloud service user account(s).

c) The Training Solution must be provided in English, and French if available, based on the choice of the user.

d) The contractor must provide a technical support number and email address that is available during core-hours. Core-hours are defined as 09:00 – 17:00 Eastern Time, Monday – Friday. Any requests outside these hours must be answered the next business day.

e) Technical Support must be provided in English, and French if available, based on the choice of the user.

f) The Training solution must be a turnkey solution, must not be a beta version of the software nor a work in progress.

g) The Contractor must provide a Production Environment:
   i. Which is available to any number of users 24 hours per day and 7 days per week.
   ii. Notification for any inaccessibility due to routine site maintenance must be provided to the Technical Authority at least two (2) days prior to it commencing.
   iii. Accessible by the Client 98.5% of the time, excluding maintenance windows.
   iv. The contractor must provide notification for all scheduled software updates at least one (1) week prior to release. Notification must include release notes and a software update schedule.
   v. Notification must be provided for all unscheduled software updates within one (1) week of release. The notification must include release notes and a software release date.

h) The contractor must be able to de-activate accounts and add new individual learner accounts as required. Maximum number of active accounts as listed in the contract.

## 6. Deliverables

| Number | Task Reference | Description of the Deliverables | Quantity and Format |
|---|---|---|---|
| **6.0** | 5.0 | Provide a web-based training solution where the software in its entirety, including all databases, hardware, and backups are provided by the Contractor outside of the RCMP network | Available to all learners identified in 5.1 to 5.4 and for RCMP Air Service administrators identified in 5.6. Accessible via Microsoft Edge, Google Chrome and Safari |
| **6.1** | 5.1 to 5.4 | Web-based Training for fixed wing and rotary pilots, Aircraft maintenance engineers and crew members | Access to web-based learning for up to 165 learners. |
| **6.2** | 5.5 | Web-based Occupational Health and Safety training for all learners | Access to web-based topics for all learners identified in 5.1 to 5.4 |
| **6.3** | 5.1 to 5.5 | An exam must be provided for each module found within each training topic | One exam per module per training topic for up to 165 learners |
| **6.4** | 5.6.b | Access to the web-based training records of RCMP employees by RCMP Air Service administrators | Administrator role for 10 RCMP Air Service administrators |
| **6.5** | 5.6.f | Annual review report | Email a review document at the end of each contract period. |
| **6.6** | 5.6.g | Email notifications | Email notifications when a topic has been assigned to a learner; and<br>Email notifications to learners and administrators when a topic is overdue as defined in 5.6 (g). |

## 7. DATE OF DELIVERY

| Deliverable | Delivery date |
|---|---|
| **6.0** | Start of contract |
| **6.1** | Within 5 business days of receiving learner information |
| **6.2** | Within 5 business days of receiving learner information |
| **6.3** | Upon learner completing module |
| **6.4** | Start of contract |
| **6.5** | 12 months after start of contract |
| **6.6** | Email notification within 2 days of a topic becoming available. |
| | Email notification within 2 weeks of a topic becoming overdue. |

## 8. Language of Work

The language of all work and deliverables must be English, and French if available.

## 9. Location of Work

Not required – web-based requirement only

## 10. Travel

The Contractor is not required to travel under this Contract.

## 11. MEETINGS

1. Initial consultation with the Contractor via teleconference to review the service. Some discussion items:
   - Learner group topic selection for the current period.
   - Learner group topic delivery schedule and validity period
   - Demonstration of the functionality of the administrator's access and tools
   - Annual report content
2. Annual meeting to discuss subsequent period's learner group topics.

## 12. SUPPORT PROVIDED BY RCMP

a) The RCMP will provide employee names and work email addresses for learner and administrator access within 1 week of contract award.
b) The RCMP will provide copies of the Operation Manuals identified in Section 4.

## ANNEX B - BASIS OF PAYMENT

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm unit price, as specified below for a cost of $_____ **(to be inserted at contract award)**. Customs duties are included and Applicable Taxes are extra.

**FOR EVALUATION PURPOSES ONLY**

Bidders must enter their firm unit prices in CAD$ in columns B, C, D, E and F and then complete the extended price for each in column G in the table below for the initial contract period and each option period.

Bidders must complete all sections of the table. Failure to complete all sections of the table may result in the bid being rejected and given no further consideration.

***Note:** The inclusion of volumetric data (estimated number of learners) in this document does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

**Financial evaluation calculation = Sum Total of Column G**

| | **Estimated Number of Learners * (A)** | **Initial contract period From: ____ To: _____ (B)** | **Option period 1 From: ____ To: _____ (C)** | **Option period 2 From: ____ To: _____ (D)** | **Option period 3 From: ____ To: _____ (E)** | **Option period 4 From: ____ To: _____ (F)** | **Estimated Price (G=AxB+ AxC+ AxD+ AxE+ AxF)** |
|---|---|---|---|---|---|---|---|
| Fixed Wing Pilots | **50** | $ | $ | $ | $ | $ | **G1** |
| Rotary Wing Pilots | **20** | $ | $ | $ | $ | $ | **G2** |
| Aircraft Maintenance Engineers | **45** | $ | $ | $ | $ | $ | **G3** |
| Crew Members | **50** | $ | $ | $ | $ | $ | **G4** |
| | | | | | | **TOTAL FOR EVALUATION PURPOSES (G1+G2+GC+G4)** | |

## ANNEX C - SECURITY REQUIREMENTS CHECK LIST (SRCL) & SECURITY GUIDE

Government of Canada | Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| 202105319 |
| 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 |
|---|---|
| RCMP | Air Services Branch |
| 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
Aviation On-Line Training for pilots, aircraft maintenance engineers and flight crew members. This will be third party cloud based content accessible by air service employees.
Formation en ligne sur l'aviation pour les pilotes, les techniciens d'entretien d'aéronefs et les membres d'équipage. Il s'agira d'un contenu sur le nuage offert par un tiers et accessible par les employés du Service de l'air.

| | | |
|---|---|---|
| 5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées? | ☑ No Non | ☐ Yes Oui |
| 5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? | ☑ No Non | ☐ Yes Oui |

6. Indicate the type of access required / Indiquer le type d'accès requis

| | | |
|---|---|---|
| 6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) | ☑ No Non | ☐ Yes Oui |
| 6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. | ☑ No Non | ☐ Yes Oui |
| 6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? | ☑ No Non | ☐ Yes Oui |

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

| Canada ☐ | NATO / OTAN ☐ | Foreign / Étranger ☐ |
|---|---|---|

7. b) Release restrictions / Restrictions relatives à la diffusion

| | | |
|---|---|---|
| No release restrictions / Aucune restriction relative à la diffusion ☐ | All NATO countries / Tous les pays de l'OTAN ☐ | No release restrictions / Aucune restriction relative à la diffusion ☐ |
| Not releasable / À ne pas diffuser ☐ | | |
| Restricted to: / Limité à : ☐ | Restricted to: / Limité à : ☐ | Restricted to: / Limité à : ☐ |
| Specify country(ies): / Préciser le(s) pays : | Specify country(ies): / Préciser le(s) pays : | Specify country(ies): / Préciser le(s) pays : |

7. c) Level of information / Niveau d'information

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

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada | Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| 202105319 |
| 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? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

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

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

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

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

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

Special comments: No security required for persec. IT requirements please see Security Guide
Commentaires spéciaux : Aucune sécurité n'est requise pour l'outil Persec. Exigences en matière de technologies de l'information : voir le Guide de sécurité.

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

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

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

**INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS**

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

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

**PRODUCTION**

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

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

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

Government of Canada | Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| 202105319 |
| 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 Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

**SUMMARY CHART / TABLEAU RÉCAPITULATIF**

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

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

# SRCL Security Guide

Air Services Branch Online Training
SRCL #: 202105319

Prepared by:
Departmental Security
Royal Canadian Mounted Police

# 1. Preamble

1.1. All contract statements and appendices within this SRCL Security Guide are only applicable to this contract.

1.2. All Contractors employed on this contract must support and maintain the security environment of the Royal Canadian Mounted Police (RCMP) by complying with the requirements described in this document. More comprehensive security obligations will be provided at the Request for a Proposal phase if applicable. This security guide only covers services or personnel storing or processing sensitive information up to the unclassified level.

# 2. Definitions

**Cloud Computing** is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Cloud Service Provider (CSP)** is an entity (can include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) that is the originator of the Public Cloud Service in its entirety.

**Compromise** is a breach of government security which includes, but is not limited to:

- unauthorized access to, disclosure, modification, use, interruption, removal, or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value;
- any action, conduct, threat or gesture of a person toward an employee in the workplace or an individual within federal facilities that caused harm or injury to that employee or individual; and,
- events causing a loss of integrity or availability of government services or activities.

**Contractor** is the entity (can include one or more natural persons, corporations, partnerships, limited liability partnerships, service providers, vendors, etc.) delivering the services to the RCMP and its partners. It is the entity approved and referenced as the 'Contractor' on the Resulting Contract.

**End User** is any individual, or system process acting on behalf of an individual, authorized by RCMP to access the Cloud Services.

**Information Spillage** refers to incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (e.g. ITSG-33, IR-9).

**Master Account** is an account with root level privileges to generate client accounts or sub-accounts that will enable departmental access to commercially available public cloud services.

**Metadata** is information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

**Organizational Data** is information or data, including all text, sound, video, or image files, log data, user names and passwords, software and related metadata, regardless of form or format: (A) disclosed by RCMP personnel, clients, partners, joint venture participants, licensors, vendors or; (B) disclosed by End Users of the Cloud Services; or (C) collected, used, processed by, or stored within the Cloud Services; which is directly or indirectly disclosed to the Contractor or Subcontractors by or on behalf of the RCMP or through the use of the Cloud Services including any such information or data to which (i) the Contractor or any Subcontractors obtains access, intentionally or inadvertently; (ii) resident on any network, System or Hardware used or managed for the RCMP by the Contractor for the Cloud Services and Contractor's services, including Contractor Infrastructure.

**Personal Information** is information about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. Examples include, but are not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual.

**Project Authority** is the entity responsible for the management of the contract. Any changes to the contract must be authorized in writing by the Project Authority, and the contractor must not perform work in excess or outside of the scope of the contract based on verbal or written requests or instructions from anyone other than the Project Authority.

**Protected B information** applies to information or assets that, if compromised could cause serious injury to an individual, organization or government.

**Protected Information** means information or assets that if compromised, could reasonably be expected to cause injury to a non-national interest – that is, an individual interest such as a person or an organization.

**Record** is any hard copy document or any data in a machine-readable format containing Personal Information

**Security Authority** is the entity within an organization who is authorized to approve contract security and retains the Security Requirements Checklist (SRCL) signing authority.

**Security Clearance** means the necessary security clearance, such as Enhanced Reliability Status or Secret Clearance, designated by Departmental Security of the RCMP, which may include some or all of the security screening steps listed in the appropriate Security Clause.

**Security Event** is any event, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents.

**Security Incident** is any event (or collection of events), act, omission or situation that has resulted in a compromise. Examples of cyber security incidents: Active exploitation of one or more identified vulnerabilities, exfiltration of data, failure of a security control, breach of a cloud-hosted or managed Government of Canada (GC) service, etc.

**Sub-contractor** is any person to whom the Contractor subcontracts the performance of the Contractor's services, in whole or in part.

**Sub-Processor** is any a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller or Contractor.

**Telework** is an agreement between a Contractors' employee and the Project Authority to carry out some or all of their work duties from a remote location. Telework requires the completion of a telework agreement between the Contractor and the Project Authority.

# 3. General Security Requirements

3.1. All Organizational Data, including hard copy documentation, or other sensitive assets for which the RCMP is responsible will be shared with the Contractor through pre-approved processes.

3.2. The information disclosed by the RCMP will be administered, maintained, and disposed of in accordance with the full Contract.

3.3. The Contractor will promptly notify the RCMP Security Authority of any security incidents related to Organizational Data or personnel in their employ.

3.4. Photography is not permitted within RCMP facilities. If photos are required, please contact the Project Authority and Departmental Security.

3.5. The Contractor is not permitted to disclose any Organizational Data or ancillary information provided by the RCMP, to any sub-contractors or sub-processors without RCMP security assessment and authorization (SA&A).

3.6. The RCMP's Departmental Security reserves the right to conduct inspections and/or security review of the Contractors' facility(ies) and/or personnel work location(s) and provide direction on mandatory safeguards (safeguards as specified in this document and possibly additional site specific safeguards). Inspections may be performed prior to sensitive information being shared and/or as required (e.g. In the event that the Contractor's office relocates). The intent of the inspection(s) is to ensure the robustness of the required security safeguards is maintained.

3.7. All Organizational Data must be protected through Cryptographic means. Cryptographic algorithms and cryptographic key sizes and crypto periods in use must align with ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions.

3.8. All voice communication, including recordings, by any cellular or mobile telephone must be restricted to non-sensitive information, unless the phone is specifically accredited and issued for sensitive information.

3.9. Prior to the authorization of a telework location, all security safeguards or mitigations identified as part of an RCMP security assessment must be adhered to.

# 4. Physical Security

## 4.1. *Storage*

4.1.1. While conducting work within the Contractor's facility, Organizational Data and Assets must be stored in a container approved by the RCMP Security Authority. The container must be located (at minimum) within an "Operations Zone". As such, the Contractors' facility(ies) must have an area/room that meets the following criteria:

| **Operations Zone** | |
|---|---|
| a) Definition | 1) An area where access is limited to personnel who are:<br>i) authorized to work there<br>ii) visitors with appropriate escorts at all times |
| b) Perimeter | 1) Must be indicated by a recognizable perimeter or a secure perimeter depending on project needs. For example, the controls may be a locked office or suite.<br>2) The work area may be subject to review by Physical Security Unit, and may also require additional safeguards or escalation as deemed necessary by the Physical Security Unit of the RCMP based on the assessment of the space, surrounding areas, site-specific conditions, etc. |
| c) Monitoring | 1) Monitored periodically by authorized personnel. For example, users of the space working at the location are able to observe if there has been a breach of security. |

Note: Refer to the Appendix A for more information on the Security Zone concept.

4.1.2. Where Contractors are permitted to work from a telework location, unencrypted or hardcopy sensitive Organizational Data is not permitted. Any RCMP assets must be stored in an area that meets the following criteria:

| **Telework Area** | |
|---|---|
| a) Definition | 1) An area within Canada* where access is limited to personnel supporting the contract and to escorted visitors. |
| b) Perimeter | 1) Where contractors are working from a telework area, the work must be conducted within a dedicated space, which can be secured from oversight and overhearing by co-habitants and windows. |
| c) Monitoring | 1) RCMP Information and assets must be monitored regularly by the Contractor. For example, users of the space working at the location are able to observe and report if there has been a breach of security. |

**Telework Area must reside within in Canada. Exceptions for Telework outside of Canada may be permitted from Five Eyes countries with an RCMP security assessment and written RCMP approval from Chief Security Officer (CSO) or delegate.*

4.1.3. For Telework locations, the Contractor must take reasonable care to protect information and assets against unauthorized disclosure, loss, theft, fire, destruction, damage or modification

4.1.4. Telework locations are only to be in enclosed and private areas, never outside or in a public venue.

4.1.5. While working, Contractors must be aware of their surroundings at all times, and be able to immediately close any programs or applications, and to lock the computer if required.

## 4.2. *Discussions*

4.2.1. Where sensitive conversations are anticipated within a Contractors' facility(ies), Operations Zones must have continuous acoustic barriers that extend from slab to slab and are acoustically rated to a level commensurate with safeguarding the sensitivity of the conversation.

## 4.3. *Production of Hard Copy Information or Other Assets*

4.3.1. The production (generation and/or modification) of hard copy Organizational Data or assets must occur in an area that meets the criteria of an Operations Zone. For further details, refer to the section Printing, Scanning, and Photocopying.

## 4.4. *Destruction*

4.4.1. Should the Contractor create any paper documentation containing Organizational Data during the term of this contract, all drafts or misprints (damaged copies and/or left over copies) must be destroyed by the Contractor.

4.4.2. Organizational Data stored in transitory or temporary storage must also be destroyed when no longer in use.

4.4.3. Organizational Data must be destroyed by the contractor following the guidance below:

a) The equipment/system (i.e. shredder) used to destroy sensitive material is rated according to the degree of destruction. In accordance with Equipment Selection Guide for Paper Shredders Equipment Selection Guide for Paper Shredders (rcmp-grc.gc.ca)

b) Any sensitive drafts/misprints awaiting disposal must be protected in accordance with its security categorization until destroyed.

## 4.5. *Transport/Transmittal of Physical Assets*

4.5.1. The physical exchange of sensitive hardcopy information and assets must be secured before transport and transmittal. When a delivery service is used, it must offer proof of mailing as well as a record while in transit and of delivery.

| | |
|---|---|
| a) Transport | 1) Transport: to transfer sensitive hardcopy information and assets up to and including Protected B from one person or place to another by someone **with a need to know** the information or need to access the asset.<br>2) Preparation: Single Envelope, Gum Seal or locked briefcase or other container of equal or greater strength.<br>3) Delivery Method: Authorized personnel. |
| b) Transmittal | 1) Transmit: to transfer sensitive information and assets up to and including Protected B from one person or place to another by someone **without a need to know** the information or need to access the asset.<br>2) Address in a nonspecific manner. Add "To Be Opened Only By" because of the need-to-know or need-to-access principles when warranted.<br>3) Preparation: Single envelope, Gum Seal<br>4) Delivery Method: Registered Mail, Priority Post, Commercial Courier or First Class Mail. |

# 5. General IT Security Controls

## 5.1. *Flow-Down of Security Obligations*

5.1.1. The security obligations apply to the Contractor and to any Sub-Contractor and/or Sub-Processors to the extent applicable. The Contractor is accountable to ensure their Sub-Contractors and/or Sub-Processors comply with these security obligations when applicable.

## 5.2. *Roles and Responsibilities for Security*

5.2.1. The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the solution between the Contractor and the RCMP. This includes, at a minimum, the roles and responsibilities for:

a) account management;
b) boundary protection;
c) asset and information system backup;
d) incident management;
e) system monitoring; and
f) vulnerability management.

## 5.3. *Use of Sub-Contractors, Sub-processors and/or Sub-sub-processors*

5.3.1. The Contractor must provide a list of sub-contractors, sub-processors and sub-sub-processors that could be used to perform any part of the work in providing the RCMP with the Service or that are related to an investigation of a Security Event or Incident that may have an impact on or to RCMP Organizational Data. The list must include the following information:

a) The name of the sub-contractors, sub-processors and/or sub-sub-processors; and
b) The identification of the work that would be performed or service provided by the sub-contractors, sub-processors and/or sub-sub-processors; and
c) the location(s) where the sub-contractors, sub-processors and/or sub-sub-processors would perform the work.

5.3.2. The Contractor must provide a list of sub-contractors, sub-processors and/or sub-sub-processors within ten days of the effective date of the Contract.

5.3.3. The Contractor must provide the RCMP notice of any new sub-contractors, sub-processors and/or sub-sub-processors at least 14-days in advance of providing that sub-contractors, sub-processors and/or sub-sub-processors with access to any Organizational Data.

## 5.4. *Telework Management*

5.4.1. The work locations of all Contractor personnel are to be clearly stated in the Classification Guide and Statement of Work (SOW). The contractor must regularly report on the location of work including employees telework locations and the number of days worked. If the location of work is expected to change through the life of the contract, this is also required to be explicitly stated. The RCMP must be notified of any change in work location that is not indicated in the Classification Guide and SOW as it will require contract review and security approval.

5.4.2. When the use of RCMP issued equipment is required, the Project Authority and Contractor must:

a) Manage and monitor remote access by the Contractor to RCMP systems and/or Organizational Data;

b) Conduct all duties throughout the contract using the provided equipment;

c) Issue standard RCMP equipment for remote work, this includes an RCMP imaged laptop with approved full-disk encryption;

d) Utilize multi-factor authentication with standard RCMP issued credentials for all secure access requirements (e.g. VPN access);

e) Ensure Contractor has read and signed the RCMP Acceptable Use Policy;

f) Ensure RCMP equipment remains within the specified work locations at all times.

5.4.3. If the use of RCMP-provided equipment is not indicated on the SRCL, the contractor may use their own equipment provided it abides by the security requirements in the section on Endpoint Protection.

## 5.5. *Endpoint Protection*

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

## 5.6. *Cryptographic Protection*

5.6.1. Contractor personnel must:

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

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

## 5.7. *Data Protection*

5.7.1. When the use of RCMP-provided equipment is required, all duties assigned to the Contractor are required to be completed using the provided equipment and follow RCMP guidance on Telework Management. Contractor personnel are not permitted to use any non-approved software, services or equipment not provided by the RCMP unless otherwise stated in writing. If the use of RCMP-provided equipment is not required, the Contractor may use their own equipment provided it abides by the security requirements in the section on Endpoint Protection.

5.7.2. Organizational Data is not to be stored on Cloud Services unless the service has been issued an Authority to Operate (ATO) by RCMP Departmental Security. The Project Authority is responsible for ensuring an ATO has been issued and all conditions are being followed throughout the life of the contract.

5.7.3. All Organizational Data at Rest hosted in a cloud service is required to implement encryption that meets RCMP requirements, this includes any and all metadata or logs derived from or related to Organizational Data.

5.7.4. Any backup of Organizational Data is subject to the same security guidelines for encryption and access controls as the primary data source.

5.7.5. Electronic records and media devices must be sanitized and/or destroyed according to ITSP.40.006 IT Media Sanitization (refer to https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006 for further information).

5.7.6. It is not permitted for either the Contractor and/or Contractor personnel to make any copies of databases or any part of those databases containing Organizational Data outside of regular service resilience capabilities and within RCMP approved regional spaces or zones.

5.7.7. The Contractor and/or Contractor personnel must not move or transmit Organizational Data at Rest outside of agreed upon service regions except when approval is obtained from RCMP.

5.7.8. The Contractor must:

a) Implement end-to-end encryption for all protected data in transit to and from any cloud services. All encryption of data-in-transit must meet the requirements of ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111);

b) Implement encryption of data at rest for all Services hosting Organizational Data, including any and all metadata or logs derived from or related to Organizational Data, where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, as specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111);

c) Implement security controls that restricts administrative access to Organizational Data, including any and all metadata or logs derived from or related to Organizational Data and Systems by the Contractor and provides the ability to require the approval of RCMP before they can access Organizational Data to perform support, maintenance, or operational activities.

d) Take reasonable measures to ensure that Contractor personnel do not have standing or ongoing access rights to Organizational Data without a need-to-know, including resources that provide technical or customer support based on approval from the RCMP.

e) Prevent any Contractor personnel from holding credentials that allow that personnel to delete, modify or copy Organizational Data, unless that person has been cleared by the RCMP to the appropriate level deemed required by the RCMP.

## 5.8. *Data Location (Residency)*

5.8.1. All sensitive Organizational Data, including data in back-ups or data maintained for redundancy purposes must be within the geographical boundaries of Canada, or a Government of Canada embassy or consulate located abroad.

## 5.9. *Data Processing*

5.9.1. All sensitive Organizational Data handled by the Contractor must be processed within the geographical boundaries of Canada*.

* Exceptions for processing Protected A Organizational Data outside of Canada may be permitted from within Five Eyes countries with an RCMP security assessment and written RCMP approval from Chief Security Officer (CSO) or delegate.

## 5.10. *Data Transport/Transmittal*

5.10.1. If there is a requirement to transport Organizational Data, it must be transported using a FIPS 140-2 Level 2, or higher, compliant portable storage device provided by the RCMP. Access to this device must be restricted to appropriately security cleared Contractor personnel only, as well as the RCMP client. The FIPS 140-2 Level 2 compliant portable storage device must be delivered by-hand or shipped following the Physical Security - Transport/Transmittal section.

5.10.2. The password for the portable storage device is to be provided via out-of-band means, either in person or by telephone to appropriately security cleared Contractor personnel only.

5.10.3. Where there is a requirement to transmit Organizational Data, including any and all metadata or logs derived from or related to Organizational Data it must be done in a secure manner including the implementation of encryption for data in transit as outlined in the section on Cryptographic Protection.

## 5.11. *Data Disposition and Returning of Records*

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

a) IT Media Sanitization ITSP.400.006 V2 (CCCS); or

b) Guidelines for Media Sanitization (NIST SP 800-88); or

c) Upon request of the RCMP, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

5.11.2. The Contractor must provide the RCMP with confirmation through a letter of attestation or log entries, that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once the RCMP discontinues its use of the Services. The RCMP may require proof that encryption keys have been destroyed or that data has been successfully crypto-shredded to prevent the recovery of data.

5.11.3. In the event of Contract Termination or when otherwise requested by the RCMP, the Contractor must:

a) Maintain all data protection and security controls at the same level detailed these Security Requirements during the period where the RCMP is recovering Organizational Data; and

b) Provide the RCMP with access to its Organizational Data for a period of time that enables the RCMP to recover all Organizational Data from the Contractor.

## 5.12. *Security Incident Response*

5.12.1. NIST defines a Security Incident as: "*An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."* In light of this, the Contractor must alert and promptly notify the RCMP Security Authority (via phone and/or email) of any compromise, breach or of any evidence such as:

a) a security incident;

b) a security malfunction in any asset;

c) data spillage;

d) irregular or unauthorized access to any asset;

e) large scale copying of an information asset; or

f) Any other irregular activity identified by the Contractor that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function.

5.12.2. If the Contractor becomes aware of or determines a compromise or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must immediately or at least no later than within 24 hours:

a) Notify the RCMP Security Authority of the Security Incident;

b) Investigate the Security Incident and provide the RCMP with detailed information about the Security Incident; and

c) Take reasonable steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

## 5.13. *Printing, Scanning, and Photocopying*

5.13.1. Printing, scanning, and/or photocopying sensitive Organizational Data must be pre-authorized by the RCMP.

5.13.2. When printing/scanning/photocopying is authorized, the Contractor must:

a) Have additional/dedicated printers/scanners/photocopiers that are not directly connected to any network including the internet. Dedicated local connections of these devices to the Contractors end-point(s) is acceptable;

b) Align with the requirements identified in Physical Security section on Storage, Production of Hard Copy Information or Other Assets and Destruction; and

c) Sanitize and/or destroy printing/scanning/photocopying devices (such as multi-function devices, printers, copiers) according to ITSP.40.006 IT Media Sanitization (refer to https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006 for further information).

## 5.14. *Identity and Access Management*

5.14.1. When the use of RCMP equipment is required, Contractor personnel will be assigned RCMP IAM credentials enabling them to access Protected RCMP assets. RCMP IAM credentials are only to be used in the course of executing the tasks outlined in contracting documentation and are to be revoked at the completion of this contract.

## 5.15. *Termination*

5.15.1. The Contractor must have implemented a documented termination or change of status procedure for personnel. The procedure, at a minimum, must include:

a) Notification of Termination to the Project Authority within the same day of termination;

b) Removal of information system access within same day of termination;

c) Termination and/or revoke any authenticators and/or credentials associated with the individual within 24 hours;

d) Conduct exit interviews that include a discussion of items identified in the TBS Standard on Security Screening and any related provisions of the Industrial Security Program;

e) Submit 330-47 Security Briefing Form for termination of contractor's security clearance;

f) Retrieve all security-related RCMP information system-related property, including access cards within 24 hours; and

g) Retain access to RCMP information and information systems formerly controlled by terminated individual.

5.15.2. Contractor personnel, upon termination of the contract for any reason, are required to return to the Project Authority all RCMP issued devices including, but not limited to:

a) Laptops;

b) Cellular Phones;

c) USB Drives; or

d) Smart Cards

# 6. SaaS/PaaS Security Obligations

*The following are additional security obligations that must be adhered to when a Contractor or Contract involves the use or development of Software as a Service (SaaS) or non-RCMP controlled Platform as a Service (PaaS) environments for the delivery of contract Services.*

## 6.1. *Network and Communications Security*

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

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

6.1.3. Use correctly configured certificates within the TLS connections in accordance with CSE guidance, CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062)

6.1.4. Ensure they can work with the RCMP's CASB solution.

## 6.2. *Secure Development*

6.2.1. When applicable, the Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as:

a) NIST;

b) ISO 27034;

c) ITSG-33;

d) SAFECode; or

e) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS); or

f) Equivalent standard approved by the RCMP in writing.

6.2.2. Upon request of the RCMP, Contractors must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

6.2.3. The Contractor shall identify, in writing, the person who will be responsible for overall security of the application development, management and that update processes throughout the Contract period.

6.2.4. Contractor personnel working on RCMP IT assets in the RCMP development environment are required to follow RCMP development processes and adhere to all RCMP IM/IT governance structures.

## 6.3. *IT Security Assessment and Authorization Process*

6.3.1. When applicable, the Contractor must demonstrate compliance with the security requirements selected by the RCMP for the scope of the Services provided by the Contractor. Compliance will have to be demonstrated through either the mapping of security controls to the applicable third party certifications (i.e. ISO 27001, SOC 2 Type 2). For unclassified information, validation of security controls through the provision of evidence directly to the RCMP may be acceptable (i.e. CSA CAIQ).

6.3.2. Compliance will be assessed and validated by the RCMP utilizing the RCMP's Security Assessment and Authorization Process or through a third-party process determined by the RCMP.

6.3.3. In the situation where the Contractor or the Service has been assessed and validated through the Canadian Centre for Cyber Security (CCCS) Cloud Security Contractor (CSC) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100), the Contractor must demonstrate that they participated in the process by successfully onboarding, participating in, and completing the program. This includes providing the following documentation to the RCMP:

a) A copy of the confirmation letter that indicates they have on-boarded into the program;

b) A copy of the most recent completed assessment report provided by CCCS; and

c) A copy of the most recent summary report provided by CCCS.

6.3.4. It is the Contractor's responsibility to notify the RCMP before placing any new or materially changed Systems or services into Production and, if directed by the RCMP, the Contractor must, at their expense submit to any additional security assessment processes and/or audits, deemed necessary by the RCMP.

6.3.5. Contractor personnel are required to participate in any Security Assessment and Authorization process deemed necessary by the Project Authority and/or Departmental Security.

*6.3.6.* Before any solutions developed in whole or in part by contractors are moved into a production environment, an Interim Authority to Operate (IATO) or full Authority to Operate (ATO) must be granted. Obtaining an I/ATO requires a security assessment as part of the Security Assessment and Authorization (SA&A) process, which can be initiated by contacting Departmental Security.

## 6.4. *Identity and Access Management*

6.4.1. Where the Contractor is providing a Service to the RCMP, the Contractor must adhere to the section on Identity and Access Management. If RCMP credentials are not required, the Contractor must implement the following:

a) Multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;

b) Role-based access;

c) Access controls on objects in storage; and

d) Granular authorization policies to allow or limit access.

## 6.5. *Privileged Access Management*

6.5.1. Where the Contractor or its personnel, including sub-contractors are accessing RCMP-managed services, the Contractor must allow the RCMP to manage and monitor Contractor privileged access to all services including services within any RCMP tenant;

6.5.2. Where the Contractor is not operating in an RCMP-managed tenant, the Contractor must:

a) Manage and monitor privileged access to Organizational Data in non-RCMP services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host RCMP 's services;

b) Restrict and minimize access to the services and Organizational Data to only authorized devices and End Users with an explicit need to have access;

c) Enforce and audit authorizations for access to the Services and Organizational Data;

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

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

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

g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Organizational Data;

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

i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Organizational Data;

j) Dual authorization may be required for actions deemed by the RCMP as highly sensitive and/or high risk;

k) When applicable, use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality to provide support and administration of Services and Contractor Infrastructure and that prohibit the use of USB mass storage devices;

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

m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Contractor personnel; and

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

6.5.3. Contractor personnel will be assigned roles within the RCMP infrastructure commensurate with their tasks. Under no circumstances are Contractor personnel to be provided with Master or Root account access.

## 6.6. *Master Account Management*

6.6.1. The Contractor must ensure adequate protection of the account management process used to deliver and support the Services for the RCMP. Security measures must include, but are not limited to:

a) Providing Master Account privileges solely to RCMP personnel in such a way that the vendor relinquishes all control of the service to the RCMP; or

b) Where Contractor personnel are required or desired to have access to the Master account, the Contractor must:

i) Limit access to only RCMP cleared and authorized users who are permitted by the RCMP to execute transactions and functions such as Master account creation and issuance;

ii) Ensure the separation of duties of individuals;

iii) Employ the principle of least privilege, including for specific security functions and privileged accounts;

iv) Ensure that authorized users are provided with security awareness and training as part of employment onboarding and when their roles change;

v) Create, protect and retain audit records related to the activities that support account management of Services provided to the RCMP;

vi) Provide the RCMP with reports on audited events for actions related to the issuance and management of Master accounts; and

vii) Ensure that Organizational Data is protected during and after personnel actions such as terminations and transfers.

# 7. Personnel Security

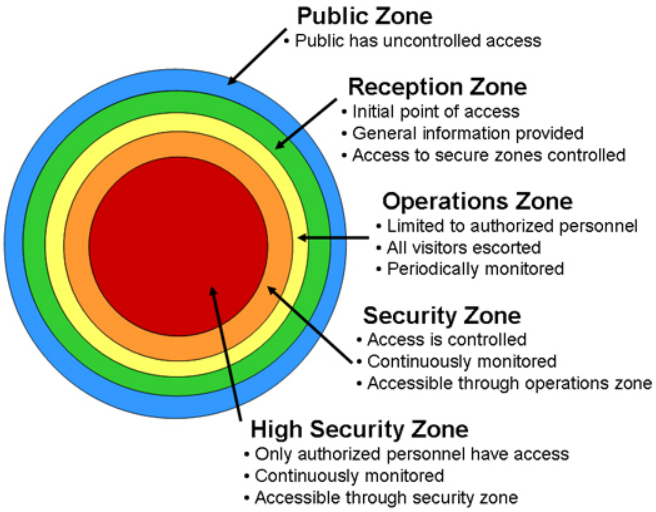
Contractor personnel will have access to RCMP sensitive information, the required RCMP Clearance or RCMP-approved equivalency* must be at the appropriate level. Contractor personnel must submit to verification by the RCMP, prior to being granted access to sensitive information, systems, assets and/or facilities. The RCMP reserves the right to deny access to any of the Contractor personnel, at any time. In the case of an Incident, security or otherwise, the RCMP has the right to deny or suspend access to RCMP locations, services and or data if situations warrant this action, pending review of the incident.

**For this requirement we have determined that no Security is required for the clearance of the personnel, but there are IT requirements involved which required security Guidance.**

# Appendix A – Security Zone Concept

The *Government Security Policy (Section 10.8 - Access Limitations)* stipulates that "departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security screening level".

The *Operational Security Standard on Physical Security (Section 6.2 - Hierarchy of Zones)* states that "departments must ensure that access to and safeguards for protected and classified assets are based on a clearly discernable hierarchy of zones".




**Public Zone** is where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings.

**Reception Zone** is where the transition from a public zone to a restricted-access area is demarcated and controlled. It is typically located at the entry to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons.

**Operations Zone** is an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored periodically. Examples: typical open office space, or typical electrical room.

**Security Zone** is an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously, i.e., 24 hours a day and 7 days a week. Example: an area where secret information is processed or stored.

**High Security Zone** is an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications recommended in the TRA, monitored continuously, i.e., 24 hours a day and 7 days a week and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel.

*Access to the zones should be based on the concept of "need to know" and restricting access to protect personnel and valuable assets. Refer to RCMP Guide G1-026, Guide to the Application of Physical Security Zones for more detailed information.*

**Annex D - Evaluation Criteria**

## 1. INSTRUCTIONS TO BIDDER

1. The Bidder is requested to provide a response to the Evaluation Criteria in the "Substantiation" column, or indicate where the criteria are met by entering the location (e.g. section/volume number, tab, page number, resume paragraph, etc.) in the "Substantiation" column.

2. For work experience to be considered by Canada, the technical bid must not simply indicate the title of a topic, but must fully describe the topic and how long it has been offered.

3. The Bidder is requested to utilize the unique item number and associated title/description of each evaluation criterion in their responses.

   Example: *M1: Topic X: Tab #3, Topic X description, Page 6, paragraph 4.*

4. Phrases such as "within the past five (5) years" used in this solicitation mean "within the five (5) years preceding the closing date of the RFP". In the event that the RFP closing date is changed after the initial publication of the RFP, the experience will be measured from the final closing date, unless otherwise directed in an RFP amendment.

5. To demonstrate the experience of the Bidder, the Bidder must provide the following details as to how the stated experience was obtained:

   i. Start and end dates (MM-YYYY) of each topic;

   ii. Reference material detailing the topics provided.

## 1. MANDATORY EVALUATION CRITERIA

In their proposals, bidders must demonstrate in writing they meet the following mandatory criteria. Failure to meet any of the mandatory criteria will render the bid non-compliant and it will be given no further consideration. Links to web pages are not accepted and will be assessed a "NOT MET" rating.

| | **CRITERIA** | **SUBSTANTIATION**<br><br>**Please Cross Reference to Specific pages in your proposal**<br>**[Completed by Bidder]** | **ASSESSMENT**<br><br>**MET/ NOT MET**<br>**[Completed by RCMP Evaluator]** |
|---|---|---|---|
| **M1** | The Bidder must demonstrate, by providing copies of previous syllabi and topics, that they have delivered a minimum of ten (10) different web-based, self-paced aviation-specific topics for at least three (3) years within the last five (5) years.<br><br>To be found compliant:<br>1. start and end dates (MM-YYYY) of each topic (spanning at least three (3) years),<br>2. each of the ten (10) topics provided as proof must be different,<br>3. topics must be from those listed in the Statement of Work. | | |

## 2. POINT-RATED EVALUATION CRITERIA

Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below.

| | POINT-RATED EVALUATION CRITERIA | Maximum | Point Breakdown Structure | SUBSTANTIATION<br><br>Please Cross Reference to Specific pages in your proposal [Completed by Bidder] | ASSESSMENT<br><br>[Completed by RCMP Evaluator] |
|---|---|---|---|---|---|
| **P1** | The Bidder should demonstrate, by providing copies of previous syllabi, courses and exams, that they can deliver the training in French. | **10** | 10 points for materials submitted in French | | |
| **P2** | The bidder should demonstrate, by providing sufficient documentation that they can provide technical support in French.<br><br>To meet this point rated criteria documentation should at a minimum provide details on the types of French technical support available (e.g. phone, email, online chat), how to contact French technical support and the hours of availability. The hours of availability at should be 09:00 – 17:00 Eastern Time, Monday – Friday | **10** | 2 points for phone support<br><br>2 points for email support<br><br>2 points for online chat support<br><br>2 points for other support options<br><br>2 points for hours of availability from 09:00 – 17:00 Eastern Time, Monday – Friday | | |
| | **TOTAL** | 20 | | | |