RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À :

kristen.scott@tc.gc.ca

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Comments – Commentaires

Proposal To: Transport Canada

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 thereof.

On behalf of the bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:

1. The bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate; and
4. If the bidder is awarded a contract, it will accept all the terms and conditions Set out in the resulting contract clauses included in the bid solicitation.

Proposition à : Transports 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 annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexées, au(x) prix indiqué(s**).**

En apposant ma signature ci-après, j'atteste, au nom du soumissionnaire, que j'ai lu la demande de propositions (DP) en entier, y compris les documents incorporés par renvoi dans la DP et que :

1. le soumissionnaire considère qu'il a les compétences et que ses produits sont en mesure de satisfaire les exigences obligatoires décrites dans la demande de soumissions;
2. cette soumission est valide pour la période exigée dans la demande de soumissions ;
3. tous les renseignements figurant dans la soumission sont complèts, véridiques et exacts; et
4. si un contrat est attribué au soumissionnaire, ce dernier se conformera à toutes les modalités énoncées dans les clauses concerrnant le contrat subséquent et comprises dans la demande de soumissions.

Title – Sujet	
Enhancing the Cybersecurity Readiness of Canada's Road Infrastructure Owner/Operators for Higher Levels of Connectivity and Automation/ Améliorer la préparation à la cybersécurité des propriétaires ou des exploitants des infrastructures routières du Canada en vue d'une meilleure connectivité et automatisation	
Solicitation No. – N° de l'invitation	**Date**
T8080-200405	January 5, 2021/le 5 janvier 2021
Client Reference No. – N° référence du client	
T8080-200405	
GETS Reference No. – N° de référence de SEAG	

Solicitation Closes **L'invitation prend fin**		**Time Zone** **Fuseau horaire**
at – à	**02 :00 PM – 14h00**	Eastern Time (ET) Heure de l'Est (HE)
on – le	**February 15, 2021/le 15 février 2021**	

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☒ **Other-Autre:** ☐

Address inquiries to – Adresser toute demande de renseignements à :	
Kristen Scott	
Area code and Telephone No. Code regional et N° de téléphone	Facsimile No. / e-mail N° de télécopieur / courriel
506-377-2564	**kristen.scott@tc.gc.ca**
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction**	
Ottawa, ON	

Instructions: See Herein
Instructions : Voir aux présentes

Delivery required -Livraison exigée	Delivery offered -Livraison proposée
See Herein – Voir aux présentes	

Jurisdiction of Contract: Province in Canada the bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)
Compétence du contrat : Province du Canada choisie par le soumissionnaire et qui aura les compétences sur tout contrat subséquent (si différente de celle précisée dans la demande)

Vendor/firm Name and Address
Raison sociale et addresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone	
e-mail - courriel	

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**

High Complexity Bid Solicitation and Resulting Contract Template (HC)

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

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

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

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

The Annexes include the Statement of Work, the Basis of Payment, the Security Requirements Checklist, the Electronic Payment Instruments, the Federal Contractors Program for Employment Equity – Certification and the Task Authorization Form.

1.2 Summary

1.2.1 Transport Canada is seeking consulting services with expertise in traffic management/critical infrastructure systems, cybersecurity assessment, auditing, risk management, penetration testing, stakeholder consultation, project management, and training course development and delivery to:

1. Develop cybersecurity profile assessment tools tailored for Traffic Management System (TMS) operations and associated infrastructure, to help road authorities evaluate their current level of cybersecurity risk management status and their target level of cybersecurity risk management status.
2. Develop guidance on creating or improving a cybersecurity risk management program for TMS operations and associated infrastructure, to help road authorities attain and maintain their targeted level of cybersecurity risk management.
3. Provide training and technical support to road authorities to perform cybersecurity assessments using the developed tools, and establish cybersecurity continuous improvement programs.
4. Provide technical support, analysis and strategic advice on an as needed basis relating to emerging cybersecurity issues in the transportation sector.
5. Perform penetration testing and vulnerability analysis on transportation sector equipment and networks on an as needed basis, to inform the management of emerging cybersecurity risks.

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

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

1.3 Debriefings

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

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

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

The 2003 (2020-05-28) 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: 120 days

2.2 Submission of Bids

Unless specified otherwise in the RFP, bids must be received by the Contract Authority by the date, time and email indicated on page 1 of the solicitation. If your bid is transmitted by electronic mail, Canada will not be responsible for late bids received at destination after the closing date and time, even if it was submitted before.

Bids must be sent by Electronic Submission to kristen.scott@tc.gc.ca

Refer to Part 3, section 3.1 “Electronic Submissions”.

2.3 Former Public Servant

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

Definitions:

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

a. an individual;

b. an individual who has incorporated;

c. a partnership made of former public servants; or

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

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

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

Former Public Servant in Receipt of a Pension:

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

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

a. name of former public servant;

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

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2019-01 and the Guidelines on the Proactive Disclosure of Contracts

2.4 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.

2.5 Applicable Laws

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

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

2.6 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least 25 days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Basis for Canada's Ownership of Intellectual Property

Transport Canada has determined that any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, for the following reasons, as set out in the ***Policy on Title to Intellectual Property Arising Under Crown Procurement Contracts***: the main purpose of the Contract, or of the deliverables contracted for, is to generate knowledge and information for public dissemination

2.8 Bid Challenge and Recourse Mechanisms

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

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

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

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

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Bid Preparation Instructions
The Bidder must submit its bid electronically. Canada requests that the Bidder submits its bid in separate documents as follows:

Section I: Technical Bid (One (1) soft copy, submitted by E-mail)
Section II: Financial Bid (One (1) soft copy, submitted by E-mail)
Section III: Certifications not included in the Technical Bid (One (1) soft copy, submitted by E-mail)

The bids must be sent by E-mail to: kristen.scott@tc.gc

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

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

Bidders must submit their financial bid in accordance with “Annex D” Pricing schedule.

3.1.1 Electronic Submission

Interested Bidders are invited to submit a proposal, through Electronic Submissions at: kristen.scott@tc.gc.ca.

Individual e-mails exceeding five megabytes (5MB), or that include other factors such as embedded macros and/or links may be rejected by the TC e-mail system and/or firewall(s) without notice to the Bidder or Contracting Authority. Larger bids may be submitted through more than one e-mail. The Contracting Authority will confirm receipt of documents. It is the Bidder’s responsibility to ensure that the Contracting Authority has received the entire submission.

Bidders should not assume that all documents have been received unless the Contracting Authority confirms receipt of each document. In order to minimize the potential for technical issues, bidders are requested to allow sufficient time before the closing time and date to confirm receipt. Technical and financial documents received after the closing time and date will not be accepted.

3.1.2 Electronic Payment of Invoices – Bid

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

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

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

Section III: Certifications
Bidders must submit the certifications and additional information required under Part 5.

Section IV: Additional Information

3.1.3 Bidder’s Proposed Sites or Premises Requiring Safeguarding Measures

3.1.3.1 As indicated in Part 6 under Security Requirements, the Bidder must provide the full addresses of the Bidder’s and proposed individuals’ sites or premises for which safeguarding measures are required for Work Performance:

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

3.1.3.2 The Company Security Officer must ensure through the Contract Security Program that the Bidder and proposed individuals hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

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 “C”.

4.1.2 Financial Evaluation

4.1.2.1 Mandatory Financial Criteria

The price of the bid will be evaluated in Canadian dollars, Applicable Taxes excluded, FOB destination, Canadian customs duties and excise taxes included.

4.2 Basis of Selection

4.2.1 A0027T Highest Combined Rating of Technical Merit and Price.
To be declared responsive, a bid must:

a. comply with all the requirements of the bid solicitation; and
b. meet all mandatory criteria;
c. obtain the required minimum of 65 points overall for the technical evaluation criteria which are subject to point rating; and
d. provide a total price for Tasks 5.1-5.5 and per diem prices for Tasks 5.6.1, 5.6.2 and 5.6.3
Note: per diem prices for each Task 5.6.1-5.6.3 may be unique for anticipated resource experience and qualification requirements, bidders should provide per diem price to cover any mix of required resources to deliver work under each Optional Task scope.

1. The rating is performed on a scale of 100 points.

2. Bids not meeting "a” or “b” or “c” will be declared non-responsive.

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

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

5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price for each group of tasks in accordance with the table below and the ratio of 30%.

Tasks	Total Per Diem Bid Price	Total Evaluated Price	Weighting	Maximum Number of Points
5.1-5.5	N/A	Total fixed evaluated price in Table A of Cost Proposal	50%	15
5.6 [(5.6.1 + 5.6.2 + 5.6.3) / 3]	Average per diem price in Table B of Cost Proposal	N/A	50%	15
Total			**100%**	**30**

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

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

Notes:
*TC may choose to terminate the evaluation upon the first finding of non-compliance.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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

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

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

5.1 Certifications Required with the Bid

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

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms for the Integrity Regime website

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

5.2 Certifications Precedent to Contract Award and Additional Information

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

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Federal Contractors Program for Employment Equity - Bid Certification

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

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

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

5.2.3 Additional Certifications Precedent to Contract Award

5.2.3.1 Status and Availability of Resources

The Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in its bid, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and

provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, maternity and parental leave, retirement, resignation, dismissal for cause or termination of an agreement for default.

If the Bidder has proposed any individual who is not an employee of the Bidder, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

5.2.3.2 Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

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

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

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

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

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

    (e) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.

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

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

PART 7 - RESULTING CONTRACT CLAUSES

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

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex "A".

7.1.2 Task Authorization

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

7.1.2.1 Task Authorization Process

1. The Project Authority will provide the Contractor with a description of the task using the "Task Authorization" form specified in Annex “G”.

2. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis and methods of payment as specified in the Contract.

3. The Contractor must provide the Project Authority, within five (5) calendar days of its receipt, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract.

4. The Contractor must not commence work until a TA authorized by the Project Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

7.1.2.2 Canada's Obligation - Portion of the Work - Task Authorizations

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

7.2 Standard Clauses and Conditions

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

7.2.1 General Conditions

2035 (*2020-05-28*), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

7.2.2 Supplemental General Conditions

4007 (2010-08-16) Canada to Own Intellectual Property Rights in Foreground Information, apply to and form part of the Contract.

7.3 Security Requirements

7.3.1
The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Contract.

1. The contractor/offeror must, at all times during the performance of the contract/standing offer, hold a valid designated organization screening (DOS) with approved Document Safeguarding at the level of **protected B**, issued by the CSP of the ISS, PSPC
2. The contractor/offeror personnel requiring access to **protected/classified** information, assets or sensitive work site(s) must **each** hold a valid personnel security screening at the level of **reliability status or secret** as required, granted or approved by the CSP/ISS/PSPC
3. The contractor/offeror **must not** remove any **protected/classified** information from the identified work site(s), and the contractor/offeror must ensure that its personnel are made aware of and comply with this restriction
4. Subcontracts which contain security requirements are not to be awarded without the prior written permission of the CSP/ISS/ PSPC
5. The Contractor **must not** utilize its Information Technology systems to electronically process, produce or store **protected/classified** information until the CSP/ISS/PSPC has issued written approval. After approval has been granted or approved, these tasks may be performed up to the level of **protected B**
6. The contractor/offeror must comply with the provisions of the:
    a) Security Requirements Check List and security guide (if applicable), attached at Annex C.
    b) Industrial Security Manual (Latest Edition)

7.3.2 Contractor's Sites or Premises Requiring Safeguarding Measures

7.3.2.1 Where safeguarding measures are required in the performance of the Work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individuals' sites or premises for the following addresses:

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

7.3.2.2 The Company Security Officer must ensure through the Contract Security Program that the Contractor and individuals hold a valid security clearance at the required level.

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from date of Contract to March 31, 2024 inclusive.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to acquire the goods, services or both described at section 5.6 of the Statement of Work under the same conditions and at the prices and/or rates stated in the Contract. The option may only be exercised by the Contracting Authority and will be evidenced, for administrative purposes only, through a contract amendment.

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

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Kristen Scott
Title: Contracting Specialist
Transport Canada
95 Foundry Street
Moncton, NB E1C 5H7
Telephone: 506-377-2564
E-mail address: kristen.scott@tc.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 provided at contract award)

The Technical Authority for the Contract is:
Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: ___-___-____
Facsimile: ___-___-____
E-mail: _____.
The Technical Authority named above 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 Technical Authority, however the Technical 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 (TBD)

Name: _____
Title: _____
Organization: _____
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

For the Work described in *the statement of work* in Annex A:

In consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid firm lot prices for a total cost of $_____ (amount to be *inserted at contract award*).
Customs duties are included and Applicable Taxes are extra.

The Contractor will be paid for the Work specified in the authorized task authorization, in accordance with the Basis of payment at Annex “B”.

For the firm price portion of the Work only, 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.

No increase in the liability of Canada or in the price of the Work specified in the authorized task authorization 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 authorized, in writing, by the Contracting Authority before their incorporation into the Work

7.7.2 Milestone Payments

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

a. an accurate and complete invoice and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b. all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

7.7.3 Electronic Payment of Invoices – Contract

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

a. Visa Acquisition Card;
b. MasterCard Acquisition Card;
c. Direct Deposit (Domestic and International);
d. Electronic Data Interchange (EDI);
e. Wire Transfer (International Only);

7.7.4 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

7.7.5 Invoicing Instructions

The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed. Each invoice must be supported by:

a. a copy of time sheets to support the time claimed
b. a copy of the release document and any other documents as specified in the Contract;
c. the description and value of the milestone claimed as detailed in the Contract

Invoices must be distributed as follows:
The original and one (1) copy must be forwarded to the address shown on page 1 of the Contract for certification and payment.

7.8 Certifications and Additional Information

7.8.1 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.

7.8.2 Federal Contractors Program for Employment Equity - Default by the Contractor

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

7.9 Applicable Laws

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

7.10 Priority of Documents

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

(a) the Articles of Agreement;
(b) the supplemental general conditions 4007(2010-08-16) Canada to Own Intellectual Property Rights in Foreground Information ;
(c) the general conditions 2035 (*2020-05-28*), General Conditions - Higher Complexity - Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirements Check List;
(h) the signed Task authorizations;
(i) the Contractor's bid dated _____, (*insert date of bid*)

7.11 Insurance

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

ANNEX “A”

STATEMENT OF WORK

Enhancing the Cybersecurity Readiness of Canada’s Road Infrastructure Owner/Operators for Higher Levels of Connectivity and Automation

1 Introduction

Transport Canada is seeking consulting services to develop tools, guidance materials, training programs and provide technical assistance to support road authorities (e.g. provinces, territories, municipalities) in assessing and improving the cybersecurity posture of their Traffic Management Systems (TMS) - including Intelligent Transportation Systems (ITS). The work products will be designed to aid road authorities in managing current risks and preparing to securely integrate new technologies and higher levels of connectivity and automation (e.g. connected and automated vehicles) into their transportation systems.

2 Background

In Canada, road transportation is a shared responsibility between federal, provincial, territorial, and local (e.g. municipal) governments. Transportation infrastructure is generally owned and operated by provincial, territorial, or local governments.

Transport Canada’s mandate is to promote a safe and secure, environmentally responsible, efficient and innovative transportation system through the development and oversight of the Government of Canada’s transportation policies and programs. Transport Canada performs a range of activities in order to develop the scientific knowledge and technology required to help accomplish the department's mission and foster innovation in the Canadian transportation sector.

In 2017, Transport Canada launched the Program to Advance Connectivity and Automation in the Transportation Systems (ACATS), to help Canadian jurisdictions prepare for the array of technical, regulatory and policy issues that will emerge as a result of the introduction of Connected and Automated vehicles (CAV). The program supports research, testing, the development of codes, standards and guidance materials, as well as, capacity-building and knowledge-sharing activities. One of the focus areas of the program is enhancing the cybersecurity of smart infrastructure systems (i.e. TMS).

TMS combine Information Technology (IT), such as traffic flow monitoring software, corporate networks and payments systems, and Operational Technology (OT), such as traffic signal controllers, variable message signs, and CAV roadside units, to improve the safety and efficiency of road transportation. Some of these technologies (e.g. ramp metering and signal preemption) have been around for decades. Newer technologies like Bluetooth detection, high definition video, advanced signal controllers, and CAV roadside communications equipment, are enabling additional safety and efficiency benefits, but also introducing higher levels of connectivity and risk of cyber threats.

While some of the newer ITS technologies have been designed with cybersecurity principles in mind, many have not. In addition to vulnerabilities that may be found within the field equipment, the integration of new and legacy systems often leads to new cybersecurity vulnerabilities in the system. This is due to the widened attack surface, the IT/OT boundary, and systems integration risks. Legacy systems were often closed, not wirelessly accessible, or electro-mechanical rather than computerized; security concerns that needed to be addressed were more physical than cyber. Many of these legacy systems have been converted to be internet accessible, for example to facilitate operations and maintenance, rendering these systems vulnerable to remote cyber-attacks. Finally, the Internet of Things, deployment of CAVs, and the supporting digital infrastructure is expected to bring new connections and interfaces with risks that must be managed appropriately.

This purpose of this project is to provide infrastructure owner/operators and transportation agencies (collectively "road authorities[1]"), with a suite of cybersecurity risk assessment tools, guidance materials, training, and technical support that are highly tailored to their business needs. Specifically, the project will produce guidance that allows road authorities to establish or improve an existing cybersecurity program in accordance with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (section 3.2, steps 1-7) as well as tools that will help develop a Current Profile (step 3) and Target Profile (step 5).
This project is expected to leverage and complement existing cybersecurity research, standards, guidance, and tools developed for transportation and other critical infrastructure sectors. The following appendices support the SOW:

Appendix A – Definition of technical terms used in the SOW.

Appendix B – List of existing technical resources.

Appendix C – Summary of related work.

3 Objectives

Transport Canada is seeking consulting services with expertise in traffic management/critical infrastructure systems, cybersecurity assessment, auditing, risk management, penetration testing, stakeholder consultation, project management, and training course development and delivery to:

1. Develop cybersecurity profile assessment tools tailored for TMS operations and associated infrastructure, to help road authorities evaluate their current level of cybersecurity risk management status and their target level of cybersecurity risk management status.

2. Develop guidance on creating or improving a cybersecurity risk management program for TMS operations and associated infrastructure, to help road authorities attain and maintain their targeted level of cybersecurity risk management.

3. Provide training and technical support to road authorities to perform cybersecurity assessments using the developed tools, and establish cybersecurity continuous improvement programs.

4. Provide technical support, analysis and strategic advice on an as needed basis relating to emerging cybersecurity issues in the transportation sector.

5. Perform penetration testing and vulnerability analysis on transportation sector equipment and networks on an as needed basis, to inform the management of emerging cybersecurity risks.

4 Scope

4.1 Activities within scope

The following activities pertain to completing the tasks and deliverables as outlined in section 5 and 6.

4.1.1 Preparing and conducting a kickoff meeting at the beginning of the project

[1] For the purposes of this statement of work, this term refers to provincial, territorial and municipal organizations responsible for managing road infrastructure, traffic operations and transit services.

4.1.2 **Developing project plans to schedule, assign resources and accomplish tasks and deliverables;**

4.1.3 **Reviewing technical reports, technical standards, legislation, equipment specifications/manual, test procedures, and engineering literature;**

4.1.4 **Organizing, developing agendas, facilitating, gathering input and presenting project results at consultation sessions with stakeholders, in coordination with Transport Canada;**

4.1.5 **Providing summary reports of consultation sessions;**

4.1.6 **Facilitating and presenting at meetings and briefing sessions with Government of Canada management and employees to further disseminate required information;**

4.1.7 **Organizing (including arranging venue, training materials, and hospitality) and delivering training sessions;**

4.1.8 **Developing report outlines, and draft, interim, and final reports or deliverables;**

4.1.9 **Addressing and incorporating comments/input on all project deliverables (including project plans, report outlines, interim reports, final reports) from Transport Canada and other appropriate stakeholders, and providing comment resolution reports;**

4.1.10 **Developing graphics and schematics as needed in reports, presentations, and training materials;**

4.1.11 **Developing software based questionnaires and tools, including writing and maintaining source code (depending on the tool format determined by the Technical Authority);**

4.1.12 **Providing on-site technical support to stakeholders in setting-up and executing assessments, developing cybersecurity improvement programs, and assessing/testing system vulnerabilities and mitigation strategies;**

4.1.13 **Conducting penetrating testing of transportation equipment and networks with the contractors' own equipment, software and other tools, in a secure environment;**

NB: the contractor is expected to have access, directly or through subcontracting, to a range of penetration testing tools and to personnel that are able to obtain a Government of Canada security clearance at the SECRET level that will be needed to perform the analysis. Purchases of equipment to be tested will be reimbursed in accordance with Section 18.5 when preauthorized by the Transport Canada and is excluded from the competitive price of the bid;

4.1.14 **At the contractor's expense, purchase technical standards that are required to complete any of the tasks;**

4.1.15 **Travel time by the contractors' staff;**

NB: travel receipt-based costs (e.g. flights, taxis, accommodation, meals) will be reimbursed in accordance with Section 11 when preauthorized by Transport Canada and are excluded from the competitive bid price;

4.2 **Activities out of scope:**

4.2.1 **Translation of deliverables from English to French (this shall be arranged by Transport Canada, if and when needed).**

4.2.2 **Conducting simultaneous interpretation during training and consultation sessions (this shall be arranged by Transport Canada, if and when needed).**

5 Tasks/Requirements

5.1 **Project Plan**

Following the kickoff meeting, and on a weekly basis (or timing as determined in discussion with Technical Authority), update the Project Plan outlining the weekly progress on all tasks, deliverables, and the allocation of project resources. The format of the Project Plan (e.g. MS Project, Excel) will be determined in discussion with the Technical Authority.

5.2 **Literature Review, Road Transportation Cybersecurity Primer, and Briefing Materials**

5.2.1 **Review cybersecurity assessment tools and risk management frameworks applicable to the transportation sector and other critical infrastructure sectors. The review must include the documents listed in Appendix A – Technical References.**

NB: there are no formal deliverables associated with Task 5.2.1. While a summary report is not required, the contractor is expected to be familiar with these resources in order to perform the other tasks listed in this section.

5.2.2 **Develop a plan and approach to develop the tools in Task 5.2. The plan must explain how critical infrastructure cybersecurity tools and risk management frameworks will be adapted for TMS and associated infrastructure. The plan must also explain options for the cybersecurity assessment logic of the tools.**

5.2.3 **Develop a road transportation cybersecurity primer (approximately 15 pages), tailored for staff and managers in a variety of organizational roles (operations, finance, HR, policy, etc.). The primer must include a cybersecurity glossary of terms, and must explain critical issues such as:**

a) Impact of connected and automated vehicles on TMS cybersecurity and vise-versa.

b) Similarities and differences between IT and OT cybersecurity.

c) Relationship between physical and digital security.

d) Roles/responsibilities/mandates for industry and the different levels of government.

e) Impact of OT cybersecurity on different functional areas in an organization (e.g. operations, finance, HR, policy, IT, etc.).

f) Publicly available examples of cybersecurity breaches or incidents based on poor cybersecurity or vulnerabilities in the road transportation infrastructure sector.

g) Costs and risks of poor cybersecurity risk management practices.

h) Importance of developing cybersecurity policies within an organization and guidance on how to develop them.

i) Baseline threat environment of the TMS and CAVs.

j) Using a systems engineering approach to architect, design, deploy, and maintain TMS infrastructure and products (i.e. NIST 800-160 or ISO 15288).

5.2.4 **With the Technical Authority, prepare a list of twenty (20) Frequently Asked Questions (FAQ) and answers on road transportation infrastructure cybersecurity.**

5.2.5 **Prepare a briefing document (approximately two pages) and presentation (approximately 20 slides) based on the primer (5.2.3), tailored for senior executives and decision makers. The purpose of these documents is to help decision makers understand the need for investing in cybersecurity planning, resources and training within their organizations. The presentation would include some basic IT/OT cybersecurity terms and concepts, key considerations (strategic, organizational, HR, financial), and other information as needed to raise cyber awareness.**

5.2.6 **Deliver up to six (6) virtual training sessions (approximately 1 hour each including time for Q&A) for senior executives and decision makers, using the materials prepared in task 5.2.5. Refine the briefing document, presentation, and FAQ as needed.**

5.2.7 **Prepare a stand-alone recorded webinar based on the virtual training sessions, to accompany the briefing document and presentation.**

5.3 **Cybersecurity Self-Assessment Toolkit Tailored for TMS Operations and Associated Infrastructure**

Under this task, the contractor will be required to develop a Cybersecurity Self-Assessment Toolkit, comprised of assessment tools (tasks 5.3.3 and 5.3.3), and user guides for the tools (5.3.5). Additional guidance to help road authorities understand how and when to use the tools as part of a cybersecurity risk management and improvement program is described in task 5.4.
The contractor will be required to demonstrate and update the toolkit following stakeholder consultation sessions as per Task 5.5.1.

5.3.1 **Design Document & Questionnaire (Cybersecurity Current Profile Assessment Tool & Cybersecurity Target Profile Assessment Tool)**

Following the plan developed under Task 5.2.2, the contractor shall prepare and submit detailed design documents outlining the format, questions, inputs, outputs, structure, process, logic and other relevant information for the tools, prior to developing the tools.
The design documents would include all of the questions that would be included in the tools, and the logic or process map showing the relationship between the questions, user inputs, and outputs generated.

5.3.2 **Develop a Cybersecurity Current Profile Assessment Tool tailored for TMS operations and associated infrastructure. A user guide to accompany the tool must also be prepared (see 5.3.5).**

The purpose of the tool is to help road authorities identify their current cybersecurity and risk management state. This information will serve as baseline from which the organization can determine where to take action. The tool must:

a) Guide the user on prioritizing and selecting the scope of operations, systems, assets and regulatory requirements for the assessment.

b) Guide the user through a comprehensive and detailed **questionnaire** that helps an organization identify their current cybersecurity readiness state , considering at a minimum, inputs relating to the organization's:

I. business/mission objectives and priorities;
II. types of equipment and ITS services deployed including the network connection between devices and the TMS, network topology and network segmentation/safeguards with particular attention to technologies resulting in increased levels of TMS connectivity or automation;
III. threat environment;
IV. operational size and complexity;
V. legal and regulatory requirements;
VI. information sharing practices;
VII. supply chain cybersecurity requirements;
VIII. organizational constraints;
IX. Each category and subcategory in Appendix A of the NIST CSF.

c) The tool must provide selectable default (i.e. suggested) options and customizable options for the inputs from 5.3.1 (b).

d) The assessment tool must guide the user in applying principles from the NIST CSF, other resources listed in Appendix B to their operating context. For example, the assessment tool may leverage questions used in the CRR Self-Assessment Package, but the questions must be refined to help the user understand how they should be applied to TMS with illustrative examples, as appropriate.

e) The assessment tool must generate a current profile output/document and a summary report, including the following components:

I. an overview of the implementation maturity level for each NIST CSF Subcategory (e.g. not implemented, partially implemented, substantially implemented or fully implemented);
II. a quantitative assessment (e.g. rating out of 10) of the organization's overall performance in each NIST CSF Function;
III. an assessment of the organization's overall NIST Framework Implementation Tier;
IV. generate qualitative feedback statements relating to the organization's preparedness, capacity, capabilities, gaps, and recommended improvement efforts.

5.3.3 **Develop a Cybersecurity Target Profile Assessment Tool tailored for TMS operations and associated infrastructure. A user guide to accompany the tool must also be prepared (see 5.3.5).**

The purpose of this tool is to help an organization identify their *desired* (i.e. target) cybersecurity and risk management state. The tool must include:

a) An additional questionnaire that helps an organization identify their target cybersecurity and risk management state, considering at a minimum, inputs relating to the organization's:

I. desired cybersecurity outcomes;
II. risk tolerance;
III. resources;
IV. threat environment;
V. risk management strategy;
VI. risk assessment results on the Current Profile;
VII. Current Profile and NIST implementation tier;
VIII. legal and regulatory requirements;
IX. information sharing practices;
X. business/mission objectives and priorities;
XI. supply chain cybersecurity requirements;
XII. organizational constraints.

b) The tool must provide selectable default (i.e. suggested) options and customizable options for the inputs from 5.3.3 (b).

c) The tool must allow for the option to import a default Target Profile as a benchmark (that includes considerations for CAV pilot operations).

d) The assessment must guide the user in applying principles from the NIST framework and other resources listed in 5.1.1 to their operating context in the transportation sector and desired outcomes in establishing an appropriate cybersecurity Target Profile.

e) The assessment tool must generate a target profile output/document and a summary report, including the following components:

I. an overview of the NIST CSF Categories and Subcategories and the target maturity level to achieve (e.g. not implemented, partially implemented, substantially implemented or fully implemented);
II. a quantitative assessment (e.g. rating out of 10) of the organization's overall target performance in each NIST Framework Function;
III. an assessment of the organization's overall NIST CSF target Implementation Tier;
IV. generated qualitative feedback statements relating to the organization's preparedness, capacity, capabilities, gaps, and recommended improvement efforts.

5.3.4 **Common design requirements for 5.3.2 and 5.3.3**

a) The tool must function as a standalone product on a single computer (i.e. user computer) and without the need for maintenance or additional developer support over time. The tool must be user-friendly and follows User Experience (UX) best practices.

b) The Cybersecurity Current Profile Assessment Tool and the Cybersecurity Target Profile Assessment Tool may be delivered as a single combined tool as long as the requirements of 5.3.3 and 5.3.3 are met. The software/file type (e.g. Excel, Adobe Acrobat or Web-based (HTML) will be determined in discussion with the Technical Authority. **The final decision on the format rests with Transport Canada.**

c) The tool(s) must not be responsible for managing and maintaining the storage of user's data (i.e. does not store user data in a database).

d) The tool(s) must be capable of allowing users to save/export their in-progress and final assessments offline and load/import them at another time, following appropriate security standards and industry best practices as determined with the project Technical Authority.

e) The questionnaire portion of the tool(s) must be tailored and specific to TMS operations and associated infrastructure, and adapted to a level of technical detail/clear language that a typical traffic engineer or technician would be able to answer without specific knowledge on cybersecurity and information technology systems.

f) The tool(s) must allow for customization including the addition of new questions, editing of existing questions, and flexibility in selecting the scope of assessment.

5.3.5 **User Guides (Cybersecurity Current Profile Assessment Tool & Cybersecurity Target Profile Assessment Tool)**

a) Prepare and submit user guides that provide detailed instructions on using the tools (tasks 5.3.32 and 5.3.3), and provide additional clarifications or considerations when answering each question including providing illustrative examples, as appropriate, as to how that question can be applied to the TMS context. This guidance will support the user in using the tools, whereas the guidance in task 5.4 will support the user in applying information generated by the tools to establish or improve a cybersecurity program in accordance with NIST CSF 3.2.

b) The guidance must include information and best practices on how to plan, structure and perform the assessments, including setting up a cross-functional team to appropriately represent the necessary organizational groups such as business, operations, security, information technology, and maintenance.

c) The guidance must include information and best practices on how to scope the assessments into appropriate security zones in accordance with the NIST Security Assurance Level approach and Purdue Model for ICS.

d) The guidance must help the user understand and establish their threat environment (5.3.2 b III, 5.3.3 a IV).

5.4 Guidance for developing and implementing a cybersecurity improvement program for TMS operations and associated infrastructure

5.4.1 Develop guidance to provide road authorities with detailed instructions on how to develop and implement a cybersecurity program and action plan (NIST CSF 3.2 Steps 1-7).

This guidance would be based on existing resources, namely the *NIST CSF section 3.2* and *ISO 27001 Information Security Management System*, and other applicable sector best practices, and would be customized for TMS operations, infrastructure, and road authorities more generally. The *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1–General Implementation Guidance*[2] provides an example of the type of sector-specific guidance and customization sought under this task.
The guidance must provide a similar level of detail to the ISO 27002 Code of practice for information security controls but adapted to a level of technical/clear language for a typical traffic engineer or technician.
The format of the guidance (e.g. one report or a series of shorter documents) will be determined in consultation with the Technical Authority.
The guidance must include:

a) Instructions to implement each step of Section 3.2 - *Establishing or Improving a Cybersecurity Program* in version 1.1 of the NIST CSF (or the equivalent section in a more recent version should one be available).

   NB: The guidance would reference the tool developed under Task 5.3.2 in step 3, and the tool developed under Task 5.3.35.3.35.3.3 in step 5.

b) Information and best practices on how to plan, structure and perform the cybersecurity program, including setting up a cross-functional team to appropriately represent the necessary organizational groups such as business, operations, security, information technology, and maintenance.

c) Information and best practices on how to scope and orient the program (NIST CSF 3.2 Steps 1-2) for consistency with the assessments and in accordance with the NIST Security Assurance Level approach and Purdue Model for ICS.

d) Guidance and best practices on the following elements customized for TMS operations and infrastructure:

I. Asset management and maintaining architecture documentation;
II. Governance, leadership and assigning responsibility;
III. Establishing the business environment and an information security policy;
IV. Risk and vulnerabilities assessment;
V. Risk management strategy;
VI. Supply chain management;
VII. System acquisition, development, integration;
VIII. Identify management, authentication and access control;
IX. Human resources, training and awareness for various TMS operational roles;
X. Data security;
XI. Information protection processes and procedures;
XII. Physical security;
XIII. Operations security;
XIV. Communications security;
XV. Maintenance;
XVI. Protective technology;
XVII. Anomalies and event detection;
XVIII. Security continuous monitoring;
XIX. Detection processes maintenance and testing;
XX. Response planning;
XXI. Response activity communications and coordination;
XXII. Incident management;
XXIII. Business continuity management;
XXIV. Analysis of incident response and recovery;
XXV. Mitigation of event and effects;
XXVI. Recovery planning;
XXVII. Recovery activity communications and coordination;
XXVIII. Internal audit and continuous improvement.

e) Information on how to apply and analyze the outputs (Current Profile and Target Profile) of the tools (Task 5.3) compare the current and target profiles NIST CSF 3.2 (Step 3 and 5).

f) Information on how to perform a risk assessment based on the results from the Current Profile tool in accordance with NIST CSF 3.2 (Step 4).

g) Information on how to develop a prioritized action plan NIST CSF 3.2 (Step 6) to address the gaps between the Current and Target Profiles. The action plan is based on the results of

analyzing the outputs of the current profile and target profile tools as described in 5.4.1 (e) and risk assessment results in 5.4.1 (f).

h) V2X and TMS specific recommendations and guidance, including: where NIST Informative References (standards, guidelines, and practices) should be considered, how they should be applied in developing a cybersecurity improvement program (NIST CSF 3.2 Step 1-7), and applying a systems engineering approach to architect, design, deploy, and maintain TMS infrastructure and products (i.e. NIST 800-160 and ISO 15288).

i) Information on how to adapt and focus the cybersecurity improvement program to implement the action plan (NIST CSF 3.2 Step 7) from 5.3.3 (g) and interactively repeat steps 1-7 for continuous improvement.

j) A case study of a typical TMS, showing concrete examples for NIST CSF 3.2 steps 1-7, including how to apply the tools and outputs to a real world use case.

5.5 Stakeholder consultation, technical support, training, and revision of the cybersecurity assessment toolkit and cybersecurity improvement program guidance documents

Stakeholder consultation and on-site technical support sessions will be organized and used to gain user feedback on the toolkit (Task 5.3) and cybersecurity guidance (Task 5.4). The contractor will revise the cybersecurity assessment toolkit and the cybersecurity guidance documents based on lessons learned from these sessions.

5.5.1 Stakeholder consultation

Organize and lead consultation sessions with stakeholders (to be identified by Transport Canada) to present and gather feedback on the cybersecurity assessment toolkit (Task 5.3) and the cybersecurity guidance documents (Task 5.4), and gather existing cybersecurity best practices performed by stakeholders.

5.5.1.1 Conduct up to three (3) group consultation sessions (additional consultation sessions may be added as per Contract Option 1 – Task 5.6.1). Two (2) of the consultation sessions may be performed via webinar. Subject to a reduction in travel limitations caused by the COVID-19 pandemic, one of the consultation sessions would be conducted in-person at a location in Canada identified by Transport Canada. Should this not be possible, it would be conducted virtually as well. The travel costs and consultation delivery costs shall be reimbursed in accordance with Section 12 and Section 18.4, respectively.

5.5.1.2 Conduct up to fifteen (15) targeted consultation sessions (i.e. interviews with individual organizations rather than group sessions).

5.5.1.3 Develop materials including agenda and presentation slides.

5.5.2 On-site technical support

Organize, lead and provide technical support to three (3) road authorities in conducting a cybersecurity assessment using the toolkit developed in Task 5.3 and implementing a cybersecurity improvement program using the guidance documents developed in Task 5.4. The technical support may include providing additional guidance and training on use of the tools and helping with analysis specific to the TMS configuration and operations being evaluated. For each of the three (3) road authority sites, the contractor must provide a minimum of four (4) days of in-person technical support (at a location in Canada to be identified by Transport Canada) and five (5) days of additional remote technical support. The travel costs shall be reimbursed in accordance with Section 12.

5.5.3 **Cybersecurity assessment toolkit (Task 5.3) and cybersecurity guidance documents (Task 5.4) revisions**

5.5.3.1 Prepare a summary of consultation session feedback, lessons learned from implementation/support and proposed changes to the toolkit and guidance documents.

5.5.3.2 Complete the revisions to the toolkit and guidance documents as agreed to with the Technical Authority.

5.5.4 **Training**

5.5.4.1 Develop a three-day training course with associated presentation materials targeted at road authority staff (e.g. traffic/ITS engineers, transportation planners, IT technicians) in providing an overview of how to use the cybersecurity assessment toolkit (Task 5.3) and cybersecurity guidance documents (Task 5.4). The travel costs shall be reimbursed in accordance with Section 12.

5.5.4.2 Develop a virtual version of the training course that could be delivered exclusively online in 3 to 6 half-day sessions.

*5.5.4.3 Organize (including venue, audiovisual equipment, hospitality, and other logistics), facilitate, and deliver **six (6)** in-person and/or virtual training course sessions.*

Subject to a reduction in travel limitations caused by the COVID-19 pandemic, these sessions would be in person at locations (in Canada) and dates identified by Transport Canada. The travel costs shall be reimbursed in accordance with Section 12.
Each on-site training session must have capacity for up to 30 in-person participants and facilitate up to 100 additional remote participants via webinar. Each virtual training session must facilitate up to 150 remote participants.
The training session delivery costs shall be reimbursed in accordance with Section 18.

5.6 **Optional Tasks – <u>Will be Structured on the Basis of Task Authorizations</u> required on an "As Needed" Basis**

When the Technical Authority requests a project under any of the contract options, the contractor is required to be made available within two weeks' notice from Technical Authority to discuss specific tasks and deliverables.
Upon request from the Technical Authority, the contractor will submit a Scope of Work document within two weeks, including:

a) project work plan
b) project outline
c) schedule of conference calls
d) time schedules for interim and final submissions
e) project content and activities
f) budget

The Scope of Work for each project must be approved by the Contracting Authority in writing prior to the commencement of any work under these options through an approved Task Authorization (Annex G).

5.6.1 **Optional Task 1: Additional consultation, technical support and training on an "as needed" basis**

The Work requested under this option will be on an "as and when requested basis" using a Task Authorization. Work requested under this option may include additional consultation, technical support, or training as per Task 5.5 to further support the use of cybersecurity assessment toolkit (Task 5.3) and cybersecurity improvement program guidance document (Task 5.4) by Canadian stakeholders.

5.6.2 **Optional Task 2: Cybersecurity vulnerability analysis (excludes penetration testing) and strategic advice on an "as needed" basis**

The Work requested under this option will be on an "as and when requested basis" using a Task Authorization. Work under this option may include simulation, reviewing technical/equipment specifications, literature on emerging technologies, system/network architectures and providing analysis, strategic advice or reporting to Transport Canada or Transport Canada stakeholders (e.g. road authorities) on specific issues.
Deliverables may take the form of reports, briefings, fact sheets, presentations, surveys, participation in meetings, and supporting workshops/roundtables.

5.6.3 **Optional Task 3: Penetration testing, vulnerability scanning, and exploit identification of systems and equipment on an "as needed" basis**

The contractor is expected to have access to the necessary facility, expertise, and equipment to conduct work described under this option.
The Work requested under this option will be on an "as and when requested basis" using a Task Authorization. Work under this option may include penetration testing, vulnerability scanning, exploit identification, and recommendations on mitigation measures for variety of vehicular and TMS equipment (e.g. traffic signal controller, cameras and camera infrastructure, GPS and timing devices, variable speed limit signs etc.) and networks to inform guidance on mitigating cybersecurity risks.
Additional work requested under this option may also include:

a) Collecting and reviewing information to characterize the equipment and prepare for vulnerability testing;
b) Configuring vehicle and TMS sub-systems in a lab setting to prepare for testing;
c) Conducting fields testing when requested/appropriate;
d) Testing recommended mitigation measures;
e) Assessing the applicability/gaps in cybersecurity standards and protocols;
f) Developing cybersecurity test procedures.

For bid preparation purposes, the bidder may assume that purchases of equipment to best tested would be made in consultation with Transport Canada and be reimbursed in accordance with Section 20.

6 Deliverables and Project Schedule

Table 1: Project deliverables and estimated timeline/schedule as weeks from award date

Item	Task	Deliverables	Timeline (within X weeks of contract award)
Project Plan, Literature Review, Road Transportation Cybersecurity Primer, and Briefing Materials, Cybersecurity Assessment Toolkit Plan			
1	5.1	Task 5.1 - Project Management Plan	2 + ongoing updates
2	5.2	Tasks 5.2.1– 5.2.5 deliverables - **drafts**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ.	6
		TC review & feedback	9
3	5.2	Task 5.2.2– 5.2.5 deliverables - **revisions**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ. Comment resolution report.	12
		TC review & feedback	15
4	5.2	Tasks 5.2.2– 5.2.5 deliverables –**final**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ. Comment resolution report.	18
		TC review & feedback	19
5	5.2	Task 5.2.6 - 5.2.7 deliverables – 6 virtual training sessions and recorded webinar	TBC
Cybersecurity Assessment Tools			
6	5.3	Task 5.3.1 deliverables – **draft**: design document and questionnaire	23
		TC review & feedback	26
7	5.3	Task 5.3.1 deliverables – **revisions**: design document and questionnaire	28
		TC review & feedback	31
8	5.3	Task 5.3.1 deliverables – **final**: design document and questionnaire	33
		TC review & feedback	34
9	5.3	Prototype functional toolkit (Task 5.3.2 and 5.3.3), **draft** user guidance (Task 5.3.5), and toolkit demonstration via webinar.	40
		TC review & feedback	44
10	5.3	**Revised** functional toolkit (Task 5.3.2 and 5.3.3) and user guidance (Task 5.3.5), and toolkit demonstration via webinar, and comments resolution summary.	48

Item	Task	Deliverables	Timeline (within X weeks of contract award)
		TC review & feedback	52
11	5.3	**Final** functional toolkit (Task 5.3.2 and 5.3.3) and user guidance (Task 5.3.5), and toolkit demonstration via webinar, and comments resolution summary.	54
		TC review & feedback	56
Cybersecurity Self-Assessment Guidance			
12	5.4	Task 5.4.1 deliverables – **outline** of the guidance	57
		TC review & feedback	59
13	5.4	Task 5.4.1 deliverables – **draft** of the guidance	69
		TC review & feedback	72
14	5.4	Task 5.4.1 deliverables – **revised** guidance and comment resolution report.	77
		TC review & feedback	80
15	5.4	Task 5.4.1 deliverables –**final*** guidance and comment resolution report. *pre consultation	83
		TC review & feedback	84
Stakeholder consultation, On-Site Technical Support, Training			
16	5.5	Task 5.5.1.1 - **Draft** agendas and presentation slides for the consultation sessions.	85
		TC review & feedback	86
17	5.5	Task 5.5.1.1 - **Final** agendas and presentation slides for the consultation sessions.	86
		TC review & feedback	87
18	5.5	Task 5.5.1- Delivery of up to 3 group stakeholder consultation sessions and 15 individual sessions on the toolkit (Task 5.3) and guidance (Task 5.4).	89
19	5.5	Task 5.5.2 - Delivery of on-site and remote technical support for 3 road authorities.	92
20	5.5	Task 5.5.3.1 - Summary of consultation session feedback, lessons learned from implementation/support and proposed changes to the toolkit and guidance documents.	93
		TC review & feedback	94
21	5.5	Task 5.5.3.2 - **Revised** toolkit and guidance.	97
		TC review & feedback	100
22	5.5	Task 5.5.4.1-5.5.4.2 deliverables - **draft** agendas, training materials and presentation slides.	103
		TC review & feedback	106
23	5.5	Task 5.5.4.1-5.5.4.2 deliverables - **revised** agendas, training materials and presentation slides, and comment resolution report.	108

Item	Task	Deliverables	Timeline (within X weeks of contract award)
		TC review & feedback	109
24	5.5	Task 5.5.4.1-5.5.4.2 deliverables - **final** agendas, training materials and presentation slides, and comment resolution report.	111
25	5.5	Task 5.5.4.3 - Delivery of 6 training sessions.	TBC

7 Language of Work

The principal language of communications both verbally and written will be English. Transport Canada will facilitate and cover the costs when translations are required.

8 Work Location

Work will be conducted at Contractor's place of business. Travel within Canada and the United States may be required to attend meetings, lead consultation sessions, deliver training, conduct testing and provide technical support. Location of meetings, consultation sessions, training sessions and on-site technical support will be determined by the project Technical Authority.

If and when required, work that requires access or processing information classified at the Protected B level may be done at contractor's place of business after the required work areas receive clearance for such work.

If and when required, work under tasks 5.6.2 and 5.6.3 that requires access or processing information classified at the Secret level will be done at suitable Government of Canada facilities and travel will be reimbursed in accordance with section 14.

9 Format of Deliverables

Unless otherwise specified in Section 5 or 4.1, deliverables are to be provided in electronic version compatible with MS Word or MS PowerPoint in English.

Presentations, outlines, draft and final reports will be in English only.

10 Contract Period

The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

I. The "**Initial Contract Period**", which begins on the date of Contract award to March 31, 2024 (end of Tasks 5.1-5.5 as identified in Sections 5 and 6); and the period during which the Contract is extended, if Canada chooses to exercise; and.

II. Any options set out in the Optional Task 1 (Task 5.6.1), Optional Task 2 (Task 5.6.2) and Optional Task 3 (Task 5.6.3), as identified in Sections 5 and 6.

Extension Options:

Canada may exercise Optional Tasks at any time by sending a written notice to the Contractor before the expiry date of the Contract Period. Canada may exercise any combination of Optional Tasks

simultaneously. The Optional Tasks may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes, through a formal Task Authorization.

11 Level of Effort

The *estimated* level of effort for Tasks 5.1-5.5 is 560 person-days during the period from contract award until March 31, 2024.

12 Travel

Travel will be required to attend meetings, lead consultation sessions, deliver training, conduct testing and provide technical support, as outlined in Sections 5-6. Travel shall be included in the price of the contract and paid in accordance with the applicable provisions set out in the Basis of Payment.

The Contractor will be reimbursed its authorized travel expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, accommodation, and private vehicle allowances specified in Appendices B, C and D of the National Joint Council Travel Directive, and with the other provisions of the directive referring to "travellers", rather than those referring to "employees". Canada will not pay the Contractor any incidental expense allowance for authorized travel.

All travel must have the prior authorization of Transport Canada through a Travel Authorization.

All payments are subject to government audit.

NB for bid preparation:

a) The bidder should include an estimated travel cost of $25,000 for reimbursable receipt based expenses.

b) The cost of contractor staff travel time should be factored into the competitive price for Tasks 5.1-5.5 assuming two days of travel time (one day each way) for each travel instance and for each required resource. Additional staff travel time for work under the Task 5.6 options will be factored into the budget defined on an as needed basis.

13 Intellectual Property

Transport Canada has determined that any intellectual property arising from the performance of the Work under the Contract will vest in Canada, on the following grounds:

- Where the main purposes of the Crown procurement contract or of the deliverables contracted for, is to generate knowledge and information for public dissemination.

14 Confidentiality Requirement

The term "Confidential Information" means all information (whether oral, written or computerized) which is identified orally or in writing as being information of a "confidential", "restricted" or "protected" nature and shall include any excerpts of or copies made of such information and any notes made from the review of such material by the consultant.

The consultant shall:

- Not reproduce, in any form, any portion of the documentation or demonstration considered proprietary by Transport Canada or other project participants;

- Hold in strictest confidence all Confidential Information received and agrees not to disclose such information to any Person other than those direct members of the proposal response team as necessary; and
- Take all precautions in dealing with the Information so as to prevent any unauthorized person from having access to such Confidential Information.

15 Commercially Sensitive Information

The information provided as part of the process may include information that is commercially sensitive.

Any information provided as part of this process will be protected from disclosure to the extent permitted by law. The Contractor will ensure that its handling of confidential, proprietary and market sensitive data obtained from Transport Canada and other sources protects the interests of the sources.

Before receiving the data or information, the contractor must conclude a formal agreement with Transport Canada on the handling, use and final disposition of the data.

16 Security clearance requirements

Resources working on Tasks 5.1-5.5 and Task 5.6.1 may require access to protected information and assets **and therefore MUST be able to obtain Government of Canada RELIABILITY status**.

Resources working on Tasks 5.6.2 and 5.6.3 may require access to protected and/or classified information and assets **and therefore MUST be able to obtain a Government of Canada SECRET clearance and have access to a WORK SITE that is able obtain Government of Canada PROTECTED B clearance**.

17 Acceptance

All work and services shall be provided to the entire satisfaction of the Technical Authority prior to payment of invoice.

18 Management of the Project

18.1 Project Management

The contractor's Project Manager is responsible for:

- exercising project sign-off and overseeing and assuring the quality of the work and deliverables
- managing the project team during the planning, implementation and reporting phases of the work
- ensuring the project is implemented within the agreed upon time, cost and performance parameters of the contract
- reporting on progress of the project to the Technical Authority on an as needed basis and at key milestones described in the Statement of Work

18.2 Project Administration

The Technical Authority will provide feedback to the contractor on interim reports and other draft deliverables and the contractor will then incorporate feedback into its final deliverables. Any feedback on the final reports or other deliverables must be addressed and resubmitted within one week of

receipt of the comments from the Technical Authority in writing. The Technical Authority will aim to provide comments within two weeks of receipt of draft deliverables subject to operational circumstances.

All deliverables will be submitted in accordance with the timelines specified in Section 4.1. The contractor must notify the Technical Authority of any anticipated delays in submitting deliverables as soon as possible.

18.3 **Project Support**

Transport Canada will assist in identifying appropriate stakeholders and locations for the consultation sessions (Task 5.5.1), technical/cybersecurity assessment support (Task 5.5.2), and training sessions (Task 5.5.4).

18.4 **Delivery of Stakeholder Consultation and Training Sessions**

The Contractor will be reimbursed for the authorized venue, virtual meeting service, hospitality, and consultation/training material costs, to deliver the session reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead.

All hospitality and event expenditures must be in accordance with the Government of Canada Directive on Travel, Hospitality, Conference and Event Expenditures and authorized in advance by the Technical Authority.

All payments are subject to government audit.

For bid preparation, the bidder should include an estimated venue, virtual meeting service, hospitality and consultation material cost as follows:

- **Task 5.5.1 - $10,000.**
- **Task 5.5.4 - $15,000 per training session, for a total of $90,000.**

18.5 **Equipment purchased for penetration testing (Task 5.6.3)**

For the purchase of equipment for testing purposes under this task, the Contractor will be reimbursed for the authorized equipment cost reasonably and properly incurred in the performance of the Work, without any allowance` for profit and/or administrative overhead. All equipment purchases must be authorized by the Technical Authority in writing prior to purchase. **For bid preparation, the bidder should include an estimated equipment cost of $50,000.**

All payments are subject to government audit.

All devices paid under this task by the Government of Canada shall remain the property of the Government of Canada. At the completion of the testing or at a time specified by the Technical Authority, the devices shall be shipped – at the government expense – to a location as determined by the Technical Authority. The Contractor shall use the device's original packaging where possible, and pack the equipment so as to avoid damage while in transit.

19 Replacement of Resources

The Contractor must provide the services of the personnel named in the contract with the required security clearances to perform the work, unless the Contractor is unable to do so for reasons beyond his/her control.

Should the Contractor at any time be unable to provide the services of the resource(s) named in the contract, the Contractor shall be responsible for providing replacement personnel within five (5) days following the replacement notification, at the same cost, who shall be of similar or greater experience, ability and attainment and whom shall be acceptable to the Technical Authority.

In advance of the date upon which replacement resources are to commence work, the Contractor shall notify, in writing, to the Technical Authority the reason for the unavailability of the resource(s) named in the contract.

The Contractor shall then provide to the Technical Authority the name(s) of the personnel, an outline of the qualifications and experiences of the proposed replacement(s), and their Government of Canada security clearance.
Any replacement personnel will be evaluated in the same manner as per the initial evaluation criteria of the RFP, and the security requirements outlined in Section 16.

Under no circumstances shall the Contractor allow performance of the services by the replacement resources that have not been authorized by the Technical Authority.

20 Contingency

The Contractor must provide a contingency plan if, in the course of the assignment, a resource becomes unavailable due to unavoidable circumstances. This plan will assure that the deadlines of the work are respected, as requested by the Technical Authority.

No Responsibility to Pay for Work not performed due to Closure of Government Offices:

i. Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

ii. If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises.

Appendix A - Glossary

a) **Aftermarket Safety Device (ASD):** A connected device in a vehicle that operates while the vehicle is mobile, but which is not connected to the data bus of the vehicle (ARC-IT, 2020).
b) **Architecture:** A framework within which a system can be built. Requirements dictate what functionality the architecture must satisfy. An architecture functionally defines what the pieces of the system are and the information that is exchanged between them. An architecture is functionally oriented and not technology-specific which allows the architecture to remain effective over time. It defines "what must be done," not "how it will be done."
c) **Automated Vehicles (AV):** Automated Vehicle systems use in-vehicle technologies (e.g., cameras, sensors, positioning, intelligent controllers and, in some cases, connectivity) to enable vehicles to navigate while taking over some driving functions such as braking, steering and acceleration. CV data extends the situational awareness of AVs beyond the limited range, line-of-sight and reliability of their in-vehicle sensors, to provide added reassurance in situations where an AV-only system might become unreliable or fail (ARC-IT, 2020).
d) **Category:** The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.” (NIST CSF, 2020)
e) **Center-to-Field Communications:** A communication link serving stationary entities, including center physical and field based objects. It may be implemented using a variety of public or private communication networks and technologies. It can include, but is not limited to, twisted pair, coaxial cable, fiber optic, microwave relay networks, cellular, spread spectrum, etc. In center to field communication the important issue is that it serves stationary objects. Both dedicated and shared communication resources may be used. One of the types of architecture interconnects defined in the ARC-IT (ARC-IT, 2020).
f) **Connected Vehicles (CV):** A vehicle containing an OBU or ASD (ARC-IT, 2020).
g) **Critical Infrastructure:** Critical infrastructure (CI) refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence (Fundamentals of Cyber Security for Canada's CI Community, Public Safety, 2020).
h) **Cybersecurity:** The process of protecting information by preventing, detecting, and responding to attacks (NIST CSF, 2020).
i) **Data Management:** This area addresses the management of data that can be used by some or all transportation agencies and other organizations to support transportation planning, performance monitoring, safety analysis, and research. Data are collected from detectors and sensors, connected vehicles, and operational data feeds from centers (ARC-IT, 2020).
j) **Field Device:** These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSE and other wireless

communications infrastructure that provides communications between Mobile elements and fixed infrastructure (ARC-IT, 2020).

k) **Field to Vehicle Communications (also known as Infrastructure to Vehicle (I2V)):** A wireless communications channel used for close-proximity communications between vehicles and the immediate infrastructure. It supports location-specific communications for ITS capabilities such as toll collection, transit vehicle management, driver information, and automated commercial vehicle operations (ARC-IT, 2020).

l) **Framework Core:** A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References (NIST CSF, 2020).

m) **Framework Implementation Tiers:** A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk (NIST CSF, 2020).

n) **Framework Profile:** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "**Current**" Profile (the "as is" state) with a "**Target**" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The **Current Profile** can then be used to support prioritization and measurement of progress toward the **Target Profile**, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations (NIST CSF, 2020).

o) **Function**: One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover (NIST CSF, 2020).

p) **Information technology (IT):** the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

q) **Infrastructure-to-everything (I2X) communication.** The exchange of information between infrastructure and other parties, including but not limited to **infrastructure-to-vehicle**, **infrastructure -to-pedestrian**, and **infrastructure -to- infrastructure communication.**

r) **Intelligent Transportation Systems (ITS):** The system defined as the electronics, communications or information processing in transportation infrastructure used singly or integrated to improve transportation safety and mobility and enhance productivity. Intelligent transportation systems (ITS) encompass a broad range of wireless and wire line communications-based information and electronics technologies (ARC-IT, 2020).

s) **On-Board Equipment (OBE):** Computer modules, display and an OBU, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment (ARC-IT, 2020).

t) **On-Board Unit (OBU):** A V2X vehicle mounted device used to transmit and receive a variety of message traffic to and from other connected devices (other OBUs and RSUs). Among the

message types and applications supported by this device are vehicle safety messages used to exchange information on each vehicle's dynamic movements for coordination and safety (ARC-IT, 2020).

u) **Operational Technology (OT):** hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

v) **Risk Management:** The process of identifying, assessing, and responding to risk (NIST CSF, 2020).

w) **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST CSF, 2020).

x) **Road authorities**: this term refers to provincial, territorial and municipal organizations responsible for managing road infrastructure, traffic operations and transit services.

y) **Road Side Unit (RSU):** A V2X connected device that is only allowed to operate from a fixed position (which may in fact be a permanent installation or from temporary equipment brought on-site for a period of time associated with an incident, road construction, or other event). Some RSUs may have connectivity to other nodes or the Internet (ARC-IT, 2020).

z) **Subcategory:** The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated." (NIST CSF, 2020)

aa) **The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)**: ARC-IT provides a common framework for planning, defining, and integrating intelligent transportation systems. It is a mature product that reflects the contributions of a broad cross-section of the ITS community (transportation practitioners, systems engineers, system developers, technology specialists, consultants, etc.) (ARC-IT, 2020).

bb) **Traffic Management Center (TMC):** An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. (ARC-IT, 2020).

cc) **Traffic Management System (TMS):** This area addresses the management of the movement of all types of vehicles, travelers and pedestrians throughout the transportation network. It deals with information collection, dissemination, and processing for the surface transportation system. It covers both automated monitoring and control activities as well as decision-making processes (both automated and manual) that address real-time incidents and other disturbances on the transportation network, as well as managing travel demand as needed to maintain overall mobility (Architecture Reference for Cooperative and Intelligent Transportation, 2020). TMS includes: the traffic management centre, centre-to-field communications, traffic signal systems, Intelligent Transportation Systems (ITS), vehicle-to-infrastructure communication systems (V2I), I2X communication systems, Closed-Circuit Television Video (CCTV), traffic signal controllers and cabinets, dynamic message signs, Road Side Units, weigh-in-motion systems, road-weather information systems, remote processing and sensing units, other IP-addressable devices, and field communication networks (NCHRP Project 03-127, TRB, 2020).

dd) **V2X Connected Device:** Any device used to transmit to or receive messages from another device. A connected device can be sub-categorized as an OBU, ASD, or RSU (ARC-IT, 2020).

ee) **Vehicle to Vehicle Communications (V2V):** Dedicated wireless system handling high data rate, low probability of error, and line of sight communications between vehicles. Advanced vehicle services may use this link in the future to support advanced collision avoidance implementations, road condition information sharing, and active coordination to advanced control systems (ARC-IT, 2020).

ff) **Vehicle-to-everything (V2X) communication.** The exchange of information between vehicles and other parties, including but not limited to **vehicle-to-infrastructure**, **vehicle-to-pedestrian**, and **vehicle-to-vehicle communication** (TAC, 2020).

Appendix B – Technical References

a) Cybersecurity and Intelligent Transportation Systems: A Best Practice Guide, United States Department of Transportation
b) Cybersecurity Capability Maturity Model (C2M2), US Department of Energy
   I. Cybersecurity Capability Maturity Model (C2M2) Facilitator Guide, version 1.1a (or latest version at the time)
   II. Cybersecurity Capability Maturity Model (C2M2), version 1.1 (or latest version at the time)
   III. Energy Sector Cybersecurity Framework Implementation Guidance
c) Cybersecurity Framework Version 1.1 Manufacturing Profile, revision 1), National Institute of Standards and Technology, supplemental documents includes:
   I. Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance
   II. Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case
   III. Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case
d) Cybersecurity Maturity Model Certification, Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), U.S. Department of Defense
e) *Cybersecurity of Traffic Management Systems*, NCHRP Project 03-127, National Cooperative Highway Research Program, Transportation Research Board, including:
   I. Task 1 - Cybersecurity Literature Review And Efforts Report
   II. Web guidance tool: publicly available at https:\\cyberguidance.transportationops.org
f) Cybersecurity Risk Management web-based Guidance Tool, National Cooperative Highway Research Program, Transportation Research Board
g) Developing a Physical and Cyber Security Primer for Transportation Agencies, National Cooperative Highway Research Program, Transportation Research Board
h) Factor Analysis of Information Risk (FAIR), FAIR Institute
i) Framework for Improving Critical Cybersecurity, Version 1.1 (or latest version at the time), National Institute of Standards and Technology (note to also include the references to other standards in the framework)
j) ISO/IEC 27000 series Information Security Management Systems (ISMS), International Organization for Standardization, including:
   I. ISO/IEC 27000 Information Technology - Security Techniques - Information Security Management System - Overview and Vocabulary
   II. ISO/IEC 27002 Information Technology - Security techniques - Code of Practice for Information Security Controls
   III. ISO/IEC 27005 Information technology - Security techniques - Information Security Risk Management
   IV. Technology -Technology- Security techniques - Information Security Management System - Requirements
q) ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes
r) NIST Security Assurance Levels: A Vector Approach to Describing Security Requirements, James D. Gilsinn, 2010

s) NIST SP 800-160
   I. Volume 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
   II. Volume 2: Systems and software engineering—Systems life cycle processes
k) Open Security Controls Assessment Language (OSCAL), National Institute of Standards and Technology
l) Risk Management Framework for Information Systems and Organizations, Special Publication 800-37, National Institute of Standards and Technology (NIST)
m) Security 101: A Physical and Cybersecurity Primer for Transportation Agencies, National Cooperative Highway Research Program, Transportation Research Board
n) Security Assurance Levels: A Vector Approach to Describing Security Requirements, paper publication, National Institute of Standards and Technology
t) The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)
o) The Cyber Resilience Review, version February 2016, US Department of Homeland Security, including:
   I. Cyber Resilience Review **Method Description and User Guide**
   II. Cyber Resilience Review **NIST Framework Crosswalk**
   III. Cyber Resilience Review **Question Set with Guidance**
   IV. Cyber Resilience Review **Self-Assessment Package**
u) The Purdue model for Industrial control systems, Industrial Cybersecurity, Pascal Ackerman, 2017
p) US Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Evaluation Tool (CSET®)

Appendix C – Related Work Summary

- **APMA CyberKit 1.0** (https://apma.ca/apma-cyberkit-1-0-2/) Cybersecurity in the Automotive & Manufacturing Sectors is becoming increasingly critical as our industry digitizes manufacturing. The industrial ecosystem is becoming more connected to the internet and other technical systems and industries. The electronics in modern vehicles are built from components supplied by multitudes of vendors from numerous suppliers who have few to no common cybersecurity standards to adhere to, and few privacy or security provisions in their manufacturing facilities. This makes the current supply chain for vehicles extremely porous in respect to cybersecurity. Every vendor and all electronic components are a potential point of vulnerability. Using the combined knowledge and expertise of the APMA's Cybersecurity Committee (CSC), we have developed the **CyberKit 1.0** to provide all manufacturing organizations with a holistic roadmap to implement or review cybersecurity in its working environment. **CyberKit 1.0** provides a structured approach to develop a comprehensive Cyber Governance Program in your business starting with defining the ownership of Cybersecurity in your organization. It moves on to define Threat & Risk Assessment methodology and the Cyber Governance Frameworks, such as the upcoming ISO 21434 & NIST CSF, that can be implemented to assess risk and secure an organization against cyber risk.
- **Canada's Vehicle Cyber Security Guidance (**https://tc.canada.ca/en/road-transportation/innovative-technologies/automated-connected-vehicles/connected-automated-vehicle-safety-what-you-need-know#_Automated-vehicle-safety)**.** Canada's Vehicle Cyber Security Guidance was developed in close collaboration with government and industry partners. These guidelines provide a set of technology-neutral guiding principles to support industry in strengthening their vehicle cyber resilience, and are an important step towards advancing the state of vehicle cyber security in Canada. The project described in this statement of work will complement this existing guidance and focus on infrastructure.
- **DHS-CISA -** ***Cybersecurity Evaluation Tool (CSET)*** (https://us-cert.cisa.gov/ics/Assessments)**.** The web-based CSET helps infrastructure owners and operators self-assess against many critical infrastructure cybersecurity standards.
- **Information and Communications Technology Council (ICTC) -** ***Developing Cyber Talent for Canadian Critical Infrastructure – Road Transportation*** (https://www.ictc-ctic.ca/developing-cyber-talent-canadian-critical-infrastructure-road-transportation/). The report examines the demand for cybersecurity talent for Canadian road authorities. The study analyzes critical skillsets while highlighting the need for a comprehensive approach to addressing challenges related to talent acquisition and skill development within the road transportation sector.
- **ITS-JPO Cybersecurity for ITS** (https://www.its.dot.gov/about/its_jpo.htm) The ITS JPO has partnered with the Connected Vehicle Pilot sites to adapt the NIST Cybersecurity Framework for connected vehicle environments. They have provided expertise from public and private firms on user requirements and countermeasures that are critical to establishing Cybersecurity Framework guidance for the connected vehicle environment. This work was originally targeted towards developing a NIST Target Profile for CAV pilot sites and is currently being expanded to develop a NIST Target Profile for ITS.

- **Transportation Research Board (TRB) National Cooperative Highway Research Program (NCHRP) Project 03-127 - *Cybersecurity of Transportation Management Systems*** (http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179). The objective of the research was to develop guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (including traffic signal systems, intelligent transportation systems, vehicle-to-infrastructure systems (V2I), and closed-circuit television systems) and, secondarily, on informing the agency's response to an attack.
- **US Department of Homeland Security (DHS) - Critical Infrastructure Security Agency (CISA) - *Cybersecurity Resilience Review (CRR)*** (https://us-cert.cisa.gov/resources/assessments)**.** The CRR is a cybersecurity self-assessment tool for the critical infrastructure. Public Safety in Canada has produced the Canadian version of the CRR.
- **USDOT - *Penetration Testing: Best Practice Guide*** (https://rosap.ntl.bts.gov/view/dot/42461/dot_42461_DS1.pdf). The guidance includes a statement of work template for US state and local transportation agencies to procure penetration testing services.

ANNEX "B"

BASIS OF PAYMENT

METHOD OF PAYMENT

Payment for services rendered will be made upon receipt and acceptance of deliverables by the Departmental Representative, and upon receipt of detailed invoices. All payments will be contingent upon TC's satisfaction with the deliverables.

The schedule of milestones/tasks for which payments will be made in accordance with the Contract is as follows:

Fiscal year 20/21 - from contract award date to March 31, 2021

Payment	Deliverable Item	Description	Fixed price
1	1	Upon Completion and Acceptance of deliverable item 1 Task 5.1 - Project Management Plan	**$[Insert at contract award] (GST/HST extra)**
Total fixed price			**$[Insert at contract award] (GST/HST extra)**

Fiscal year 21/22 - from April 1, 2021 to March 31, 2022

Payment	Deliverable Item	Description	Fixed price
2	2	Upon Completion and Acceptance of deliverable item 2 Task 5.2.2 – 5.2.5 deliverables - **drafts**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ.	$[Insert at contract award] (GST/HST extra)
3	3-4	Upon Completion and Acceptance of deliverable items 3-4 Task 5.2.2 – 5.2.5 deliverables - **revisions**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ. Comment resolution report. Tasks 5.2.2 – 5.2.5 deliverables – **final**: toolkit plan, road transportation cybersecurity	$[Insert at contract award] (GST/HST extra)

		primer, briefing document, presentation slides, and, FAQ. Comment resolution report.	
4	5	Upon Completion and Acceptance of deliverable items 5 Task 5.2.6 - 5.2.7 deliverables – 6 virtual training sessions and recorded webinar	$[Insert at contract award] (GST/HST extra)
5	6-11	Upon Completion and Acceptance of deliverable items 6-11 Task 5.3.1 deliverables – design document and questionnaire Functional toolkit (Task 5.3.2 and 5.3.3), user guidance (Task 5.3.5), and toolkit demonstration via webinar, and comments resolution report.	$[Insert at contract award] (GST/HST extra)
Total fixed price			**$[Insert at contract award] (GST/HST extra)**

Fiscal year 22/23 - from April 1, 2022 to March 31, 2023

Payment	Deliverable Item	Description	Fixed price
6	12-15	Upon Completion and Acceptance of deliverable items 12-15 Task 5.4.1 deliverables – guidance and comment resolution report	$[Insert at contract award] (GST/HST extra)
7	16-18	Upon Completion and Acceptance of deliverable items 16-18 Task 5.5.1.1 Agendas and presentation slides for the consultation sessions. Delivery of up to 3 group stakeholder	$[Insert at contract award] (GST/HST extra)

		consultation sessions and 15 individual sessions on the toolkit (Task 5.3) and guidance (Task 5.4).	
8	19	Upon Completion and Acceptance of deliverable items 19 Task 5.5.2 - Delivery of on-site and remote technical support for 3 road authorities.	$[Insert at contract award] (GST/HST extra)
9	20-21	Upon Completion and Acceptance of deliverable items 20-21 Task 5.5.3.1 - Summary of consultation session feedback, lessons learned from implementation/support and proposed changes to the toolkit and guidance documents. Revised toolkit and guidance.	$[Insert at contract award] (GST/HST extra)
Total fixed price			**$[Insert at contract award] (GST/HST extra)**

Fiscal year 23/24 - from April 1, 2023 to March 31, 2024

Payment	Deliverable Item	Description	Fixed price
10	22-24	Upon Completion and Acceptance of deliverable items 22-24 Task 5.5.4.1-5.5.4.2 deliverables –agendas, training materials and presentation slides, and comment resolution report.	$[Insert at contract award] (GST/HST extra)
11	25	Upon Completion and Acceptance of deliverable items 25 Task 5.5.4.3 - Delivery of 6 training sessions	$[Insert at contract award] (GST/HST extra)
Total fixed price			**$[Insert at contract award] (GST/HST extra)**

1. **Professional Services (Task Authorization)**

   The Contractor will be paid for the Work specified in the authorized task authorization, in accordance with the task hourly rates detailed below:

Optional Task 5.6.1 – Additional consultation, technical support and training on an "as needed" basis for a fixed per diem price of $ **[Insert at contract award]** (GST/HST extra)

Optional Task 5.6.2 - Cybersecurity vulnerability analysis (excludes penetration testing) and strategic advice on an "as needed" basis for a fixed per diem price of $ **[Insert at contract award]** (GST/HST extra)

Optional Task 5.6.3 - Penetration testing, vulnerability scanning, and exploit identification of systems and equipment on an "as needed" basis for a fixed per diem price of $**[Insert at contract award]** (GST/HST extra)

2. Authorized Travel and Living Expenses for the Work:

Concerning the requirements to travel described in the Statement of Work in Annex A, the Contractor will be paid for its authorized travel and living expenses reasonably and properly incurred in the performance of the Work done, delivered or performed at cost, without any allowance for profit and administrative overhead, in accordance with the meal and private vehicle expenses provided in Appendices B, C and D of the National Joint Council Travel Directive; outside the National Capital Region (NCR) defined in the *National Capital Act (R.S.C., 1985, c. N-4)*, available on the Justice Website (http://laws-lois.justice.gc.ca/eng/acts/N-4/page-9.html#docCont). All travel must have the prior authorization of the Project Authority.

Canada will not accept travel and living expenses that may need to be incurred by the Contractor for any relocation of resources required to satisfy its contractual obligations." and with the other provisions of the directive referring to "travellers", rather than those referring to "employees".

Canada will not accept travel and living expenses that may need to be incurred by the Contractor for any relocation of resources required to satisfy its contractual obligations."

The authorized travel and living expenses will be paid upon submission of an itemized statement supported by receipt vouchers. All payments are subject to government audit.

ANNEX “C”

SECURITY REQUIREMENT CHECKLIST

****Attached as a separate document**

ANNEX "D"

EVALUATION PROCEDURES AND BASIS OF SELECTION

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.

Technical Evaluation

Mandatory Technical Criteria

The mandatory requirements below will be evaluated on a pass/fail (meets / does not meet) basis. Proposals that do not meet the requirements will be deemed non-responsive and given no further consideration.

Note: TC may choose to terminate the evaluation of any proposal upon the first findings of non-compliance with a mandatory requirement or upon the first finding where a proposal fails to meet a minimum score for a rated requirement.
An evaluation team composed of representatives of the Government of Canada will evaluate the proposals.

The evaluation team reserves the right but is not obliged to perform any of the following:

a) seek clarification or verify any or all information provided by the Bidder with respect to this RFP; and,
b) contact any or all of the references supplied; references are only to be contacted to validate information stated in the bid.

Mandatory Requirements

Proposals will be evaluated in accordance with the mandatory evaluation criteria as detailed herein. Bidders' Proposals must clearly demonstrate that they meet all Mandatory Requirements for the proposal to be considered for further evaluation. Proposals not meeting the mandatory criteria will be excluded from further consideration.

For any *Project Summaries* provided in demonstration of mandatory or rated experience requirements, the bidder must provide:

1. A description of the project, and the scope of services rendered, deliverables and results.
2. The value of the project
3. If applicable: A solicitation reference number or award notice, with link to government tender site
4. The scale of the project (size of the client organization, if applicable).
5. The dates and duration of the project (indicating the years/months of engagement and the start and end dates of the work).
6. A brief description of the proposed resource(s) role in the project.
7. The name of the client organization (if this can be provided).
8. Confirmation that the services rendered and deliverables met client expectations for time, budget, and quality of work.

The bidder may use an individual *project summary* to meet one or more of the mandatory or rated criteria. The bidder may choose to provide *project summaries* early in their proposal, reference these when responding to individual criteria, while providing additional clarification if needed. This will help the bidder avoid repeating the same information multiple times.

The Bidder must include the following table in their proposal, indicating that their proposal meets the mandatory criteria, and providing the proposal page number or section that contains information to verify that the criteria has been met.

Table 1: Mandatory criteria

No.	Mandatory Criteria	Meets Criteria (✓)	Proposal Page No.
M1	The Bidder's proposed resource(s) collectively **must** have completed three (3) projects within the last ten (10) years that relate to performing cybersecurity assessments on critical infrastructure systems (e.g. transportation sector, financial sector, energy sector) using recognized methodology or standards such as ISO 27001, NIST CSF or other appropriate cybersecurity standards. **Note:** This can be demonstrated as a total of 3 projects completed by one or more of the proposed resource(s). The proposed resource(s) are not required to have worked on the same projects to be counted as experience. This must be demonstrated through *project summaries* as defined in the general requirements.		
M2	The Bidder must include within their proposal a detailed curriculum vitae (CV) for each of their proposed resources for this contract and identify the role of each resource in delivering the contract. The CV for each proposed resources must include a summary/description of the previous projects/work experience for the last 10 years, and indicate when the work was carried out and for how long.		
M3	At least one proposed resource must demonstrate through their CV the following experience: • delivering presentations to large stakeholder groups (over 50 people); and		

	• leading technical working groups, task forces or other collaborative initiatives.		
M4	At least one proposed resource must demonstrate through their CV a minimum of five (5)* years of performing vulnerability analysis and penetration testing of critical infrastructure systems. This resource MUST be able to obtain a Government of Canada Secret (Level II) clearance which is required for Optional Tasks 5.6.2 and 5.6.3, as per Section 16. This requirement may be met through subcontracting resources that meet the experience and security clearance requirements. *This experience does not need to be five (5) consecutive years.		
M5	The bidder must propose a Project Manager* that has a minimum of (5)** years of project management experience. This experience must be demonstrated through their CV. *The responsibilities of the Project Manager are outlined in Section 18. **This experience does not need to be five (5) consecutive years.		
M6	The Bidder must include a draft Project Plan and description of proposed approach to meeting the task requirements and managing potential project risks. The Project Plan must specify the weekly progress targets on all tasks and deliverables as well as the allocation of each project resource(s)'s time in person-days. The Project Plan must briefly describe the role of each resource on the project.		
M7	The bidder must have access to a facility or lab to perform penetration testing relating to task 5.6.3 and must provide a description of the plan to perform work under this contract option with resources that meet mandatory requirement M4.		
M8	The technical portion of the bid must not exceed 100 pages (excluding title, table of contents, Project Plan, and CVs).		

Technical Requirements

Point Rated Technical Criteria

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

Bids must achieve an overall minimum percentage of 65%. Bids that do not meet this requirement will be declared non-responsive. Each point rated technical criterion should be addressed separately.

We advise tenderers to respond in the order that follows and in detail, to allow for a complete evaluation. The evaluation will be based solely on the information provided in the proposal. The review team may verify the information provided and obtain clarification.

Based on the Bidder's Proposal, each rated item will be allocated points on a percentage basis as follows:

Table 2: Point rated technical criteria

Rated Criteria	Point Rating	Maximum Points	Proposal Page No.
R1. Quality of Project Plan and Description of Proposed Approach			
The Bidder must include a draft Project Plan for meetings the requirements of tasks 5.1-5.5 according to the schedule in Section 6. The Bidder should also include a description of their proposed resources and approach for work under the contract options as per task 5.6. The Project Plan should specify the weekly progress targets on all tasks and deliverables as well as the allocation of each project resource(s)' time in person-days. The Project Plan should also include a description of the proposed approach to meeting the task requirements (including developing the cybersecurity toolkit and guidance documents) and managing potential project risks. For the purposes of preparing the project plan, the bidder is to assume a	No plan = 0 points Inadequate plan with inefficient detail or clarity to show task allocation amongst project resource(s) and approach to meeting deliverables, major weaknesses/gaps in information = 4 points Inadequate plan with inefficient detail or clarity to show task allocation amongst project resource(s) and approach to meeting deliverables, significant weaknesses/gaps in information = 8 points Adequate plan that provides sufficient detail to show task allocation amongst project resource(s) and realistic approach to meeting deliverables, some weaknesses/gaps in information = 12 points Good plan that provides sufficient detail to show task allocation amongst project resource(s) and realistic	20	

contract award date of February 1st, 2021.	approach to meeting deliverables, few minor weaknesses/gaps in information = 16 points Excellent and thorough plan that provides sufficient detail to show task allocation amongst project resource(s) and realistic approach to meeting deliverables; very minor gaps in information = 20 points		
R2. Work experience in conducting or guiding an organization through cybersecurity assessments or audits on critical infrastructure systems			
One or more of the proposed resources have experience in conducting, or guiding an organization through cybersecurity assessments or audits (in accordance with the NIST cybersecurity framework, ISO 27001, or another reputable framework on critical infrastructure systems (e.g. transportation sector, financial sector, energy sector etc.). This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the	**Depth of experience (maximum of 5 points) :** **1 point** per relevant project in the last 10 years where the scope of the assessment included a client with 5,000 or more employees or the assessment was multi-year**; 0.5 points** per other relevant projects in the last 10 years For a project example to be considered relevant, the Bidder **must** clearly relate how the experience of the proposed resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of 5 points) :** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates	10	

Statement of Work requirements.	to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 2 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 4 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 5 points		
R3. Work experience in developing training materials and programs as well as leading, organizing, and delivering enterprise-wide training activities relating to cybersecurity.			
One or more of the proposed resources have experience in developing training materials and programs as well as leading, organizing, and delivering enterprise-wide training activities relating to cybersecurity. This experience should be demonstrated through a	**Depth of experience (maximum of 5 points) :** **1 point** per relevant project in the last 10 years where the scope of the training program included 100 or more employees or the training program was multi-year; **0.5 points** per other relevant projects in the last 10 years For a project example to be considered relevant, the Bidder	10	

descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the Statement of Work requirements.	**must** clearly relate how the experience of the proposed resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of points) :** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 2 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 4 points		

	The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 5 points		
R4. Work experience in developing cybersecurity assessment tools and guidance documents for critical infrastructure systems			
One or more of the proposed resources have experience in developing interactive (i.e. accepts and analyses user inputs) cybersecurity assessment questionnaires or other tools similar to those described in the Statement of Work for critical infrastructure systems, as well as developing supporting guidance documents. (e.g. user guides). This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the	**Depth of experience (maximum of 5 points):** **1 point** per relevant project in the last 10 years that includes an cybersecurity assessment tool **and** guidance documentation; **0.5 points** per relevant project in the last 10 years that includes only a cybersecurity assessment tool **or** guidance documentation on completing a cybersecurity assessment For a project example to be considered relevant, the Bidder **must** clearly relate how the experience of the proposed resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of 10 points) :** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points	15	

Statement of Work requirements.	The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 6 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 8 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 10 points		
R5. Work experience in preparing deliverables for federal, provincial, territorial or state governments in Canada or the US in the form of presentations or reports.			
One or more of the proposed resources have experience in preparing	**Depth of experience (maximum of 5 points):** 1 point per relevant project	10	

deliverables for federal, provincial, territorial or state governments in Canada or the US in the form of presentations or reports. This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the Statement of Work requirements.	For a project example to be considered relevant, the Bidder **must** clearly relate how the experience of the proposed resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of 5 points) :** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 2 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to		

	meet most project requirements = 4 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 5 points		
R6. Work experience in performing technical cybersecurity vulnerability analysis and penetration testing on industrial controls systems or equipment			
One or more of the proposed resources have experience in performing hands-on cybersecurity vulnerability analysis and penetration testing on industrial controls systems or equipment, including or similar to: a) Collecting and reviewing information to characterize the equipment and prepare for vulnerability testing b) Configuring vehicle and TMS sub-systems in a lab setting to prepare for testing c) Conducting field testing d) Testing recommended mitigation measures e) Assessing the applicability/gaps in cybersecurity standards and protocols f) Developing cybersecurity test procedures g) Applying cybersecurity test standards (e.g. OWASP). h) Utilizing existing cybersecurity testing software and	**Depth of experience (maximum of 5 points):** 1 point per relevant project in the last 10 years For a project example to be considered relevant, the Bidder **must** clearly relate how the experience of the proposed resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of 5 points):** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the**	10	

frameworks (e.g. web application scanner such as OWASP Zap, vulnerability scanners, digital forensic software). This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the Statement of Work requirements.	**project requirements** = 2 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 4 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 5 points		
R7. Work experience on cybersecurity projects in the transportation sector, specifically relating to TMS, ITS or CAVs			
One or more of the proposed resources have experience working on cybersecurity projects in the transportation sector. This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in	**Depth of experience (maximum of 10 points):** **0.5 point** per relevant project in the transportation sector; **an additional 1.5 points** per relevant project specifically relating to TMS, ITS or CAVs For a project example to be considered relevant, the Bidder **must** clearly relate how the experience of the proposed	20	

the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the Statement of Work requirements.	resource(s) applies to this Statement of Work. **Relevance and scope of experience (maximum of 10 points):** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 3 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 6 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 8 points		

	The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 10 points		
R8. Work experience in leading multi-stakeholder working groups, consultations or other collaborative working initiatives			
One or more of the proposed resources have experience in leading in multi-stakeholder working groups, consultations or other collaborative working initiatives. This experience should be demonstrated through a descriptive narrative that references *project summaries*, as defined in the General Requirements section, explaining: • the role of the proposed resource(s) in the project examples; and • how the experience of the proposed resource(s) is applicable and relevant to their proposed role on the project and meeting the Statement of Work requirements.	**Relevance and scope of experience (maximum of 5 points):** The proposed resource(s)' role and experience in the described projects is **not relevant** to the Statement of Work, as it relates to this criterion; or there is **insufficient detail** demonstrating that the work experience is transferable and applicable to meet project requirements = 0 points The proposed resource(s)' role and experience in the described projects has **inadequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **few of the project requirements** = 2 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is transferable and applicable to **meet many project requirements** = 3 points	5	

	The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet most project requirements** = 4 points The proposed resource(s)' role and experience in the described projects has **adequate relevance** to the Statement of Work as it relates to this criterion; the described experience is **clearly** transferable and applicable to **meet or exceed all project requirements** = 5 points		
TOTAL RATED REQUIREMENT (MAX 100 POINTS) **PASS MARK (65% - 65 POINTS)**		**Total Points**	**/100**

ANNEX "E"

PRICING SCHEDULE

Professional Services and Associated Costs

The Contractor shall tender an all-inclusive fixed price for the conduct of all work as described in Tasks 5.1-5.5 of the Statement of Work. In addition, the Contractor shall provide a breakdown of the tendered all-inclusive fixed price in accordance with Table A

Table A – core work cost proposal

Deliverable Item	Belongs to Task	Deliverable Item Description	Fixed Evaluated Price
1	5.1	Task 5.1 - Project Management Plan	$_____ (GST/HST extra)
2	5.2	Task 5.2.2 – 5.2.5 deliverables - **drafts**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ.	$_____ (GST/HST extra)
3	5.2	Task 5.2.2 – 5.2.5 deliverables - **revisions**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ. Comment resolution report.	$_____ (GST/HST extra)
4	5.2	Tasks 5.2.2 – 5.2.5 deliverables –**final**: toolkit plan, road transportation cybersecurity primer, briefing document, presentation slides, and, FAQ. Comment resolution report.	$_____ (GST/HST extra)
5	5.2	Task 5.2.6 - 5.2.7 deliverables – 6 virtual training sessions and recorded webinar	$_____ (GST/HST extra)
6-8	5.3	Task 5.3.1 deliverables – design document and questionnaire	$_____ (GST/HST extra)
9-11	5.3	Functional toolkit (Task 5.3.2 and 5.3.3), user guidance (Task 5.3.5), toolkit demonstration via webinar, and comment resolution reports.	$_____ (GST/HST extra)
12-15	5.4	Task 5.4.1 deliverables – guidance and comment resolution report.	$_____ (GST/HST extra)

Deliverable Item	Belongs to Task	Deliverable Item Description	Fixed Evaluated Price
16-18	5.5	Task 5.5.1 - Agendas and presentation slides for the consultation sessions. Delivery of up to 3 group stakeholder consultation sessions and 15 individual sessions on the toolkit (Task 5.3) and guidance (Task 5.4).	$_____ (GST/HST extra)
19	5.5	Task 5.5.2 - Delivery of on-site and remote technical support for 3 road authorities.	$_____ (GST/HST extra)
20-21	5.5	Task 5.5.3 - Summary of consultation session feedback, lessons learned from implementation/support and proposed changes to the toolkit and guidance documents. Revised toolkit and guidance.	$_____ (GST/HST extra)
22-24	5.5	Task 5.5.4.1-5.5.4.2 deliverables – agendas, training materials and presentation slides, and comment resolution reports.	$_____ (GST/HST extra)
25	5.5	Task 5.5.4.3 - Delivery of 6 training sessions.	$_____ (GST/HST extra)
Total fixed evaluated price for core work		$_____ (GST/HST extra)	

Professional Services (Task Authorization)

The Contractor shall tender a per diem price for each Optional Task to cover work for one resource per work day. The optional work can only be started and/or paid for upon approval and completion of Task Authorization for an Optional Task(s). Please note that Optional Tasks be may invoked at any time during the contract period once the security clearance requirements have been met.

Table B – Optional work cost proposal

Optional Task	Per Diem Price (per person-day)
Optional Task 1: Task 5.6.1- Additional stakeholder consultation, on-site technical support and training on an “as needed” basis	$_____ per person-day (GST/HST extra)

Optional Task	Per Diem Price (per person-day)
Optional Task 2: Task 5.6.2 - Cybersecurity vulnerability analysis (excludes penetration testing) and strategic advice on an "as needed" basis	**$_____** per person-day **(GST/HST extra)**
Optional Task 3: Task 5.6.3 - Penetration testing, vulnerability scanning, and exploit identification of systems and equipment on an "as needed" basis	**$_____** per person-day **(GST/HST extra)**
Average per diem price for optional tasks 1, 2 and 3 (5.6.1 + 5.6.2 + 5.6.3) / 3	**$_____** per person-day **(GST/HST extra)**

Travel Receipt Based Expenses

Travel will be required to attend meetings, lead consultation sessions, deliver training, conduct testing and provide technical support, as outlined in Sections 5-6, shall be included in the price of the contract and paid in accordance with the applicable provisions set out in the Basis of Payment.
The Contractor will be reimbursed its authorized travel expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, accommodation, and private vehicle allowances specified in Appendices B, C and D of the National Joint Council Travel Directive, and with the other provisions of the directive referring to "70travelers", rather than those referring to "employees". Canada will not pay the Contractor any incidental expense allowance for authorized travel.
All travel must have the prior authorization of Transport Canada through a Travel Authorization.
All payments are subject to government audit.
The cost of contractor staff travel time should be factored into the competitive price for Tasks 5.1 -5.5. Additional staff travel time for work under the Task 5.6 options will be factored into the budget defined on an as needed basis.
Total estimated maximum travel price …… $25,000 (GST/HST extra)

Consultation and Training Receipt Based Expenses

The Contractor will be reimbursed for the authorized venue, virtual meeting service, hospitality and consultation/training material costs, to deliver the session reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead.
All hospitality and event expenditures must be in accordance with the Government of Canada Directive on Travel, Hospitality, Conference and Event Expenditures and authorized in advance by the Technical Authority.
All payments are subject to government audit.

For bid preparation, the bidder should include an estimated venue, virtual meeting service, hospitality and consultation material cost as follows:

Total estimated maximum price for task 5.5.1 …… $10,000 (GST/HST extra)

Total estimated maximum price for task 5.5.4 …… $90,000 (GST/HST extra)

Purchase of Equipment to be Tested Receipt Based Expenses

For the purchase of equipment for testing purposes as per Task 5.6.3, the Contractor will be reimbursed for the authorized equipment cost reasonably and properly incurred in the performance of the Work, without any allowance` for profit and/or administrative overhead. All equipment purchases must be authorized by the Technical Authority in writing prior to purchase.

All payments are subject to government audit.

All devices paid under this task by the Government of Canada shall remain the property of the Government of Canada. At the completion of the testing or at a time specified by the Technical Authority, the devices shall be shipped – at the government expense – to a location as determined by the Technical Authority. The Contractor shall use the device's original packaging where possible, and pack the equipment so as to avoid damage while in transit.

Total estimated maximum price for task 5.6.3 …… $50,000 (GST/HST extra)

Total Tender Prices

Note: Refer to Basis of Selection section for evaluation weighting of tender prices.

Tender price for Tasks 5.1-5.5 in 2.1 (Table A) (excluding HST)	**$_____**
Tender average per Diem Price for Optional Tasks 5.6 in (Table B) (excluding HST)	**$_____**
Tender Price for Estimated Travel Costs in 2.3 (excluding HST)	**$25,000 (GST/HST extra)**
Tender Price for Estimated Consultation/Training Costs in 2.4 (excluding HST)	**$100,000 (GST/HST extra)**
Tender Price for Estimated Equipment Costs in 2.5 (excluding HST)	**$50,000 (GST/HST extra)**
Total tender price (excluding HST and per diem rates)	**$_____**

ANNEX “F” to PART 3 OF THE BID SOLICITATION

ELECTRONIC PAYMENT INSTRUMENTS

The Bidder accepts to be paid by any of the following Electronic Payment Instrument(s):

( ) VISA Acquisition Card;

( ) MasterCard Acquisition Card;

( ) Direct Deposit (Domestic and International);

( ) Electronic Data Interchange (EDI);

( ) Wire Transfer (International Only);

ANNEX "G" to PART 5 OF THE BID SOLICITATION

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

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

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

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

Complete both A and B.

A. Check only one of the following:

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

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

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

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

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

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

OR

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

B. Check only one of the following:

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

OR

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

ANNEX "H"

TASK AUTHORIZATION FORM

All invoices must show the following agreement reference numbers. Toutes les factures doivent indiquer les numéros relatifs au contrat.

Order Office - Bureau Demandeur:	X	**Contract Number - Numéro du Contrat:**	X
Financial Code(s) - Code(s) financier(s):	X	**Amount - Montant:**	**$** Includes GST
		Request Date/Date de la demande	X

To Contractor - À L'Entrepreneur: **Vendor name here** **xxxxxxxxxxxx** **BPN: 123861098PG0001** **Services for / pour:**	**To the Contractor:** **You are requested to supply the following services in accordance with the terms of the above referenced contract. Only services included in the contract shall be supplied against this requisition. Please advise the undersigned if the delivery date cannot be met. Invoices shall be prepared in accordance with the instructions set out in the contract.** **A L'Entrepreneur:** **Vous êtes prié de fournir les services suivants en conformité des terms du contrat mentionnés ci-dessus. Seuls les services mentionnés dans le contrat doivent être fournis à l-appui de cette demande. Prière d'aviser le signataire si la livraison ne peut se faire dans les délais prescrits. Les factures doivent être établies selon les instructions énoncées dans le contrat.**

Contract Item - No. d' article du contrat	Services (Resources)	Category	$Rate $Taux		$Amount $Montant
			$		[redacted]
			$		[redacted]
				TOTAL	$0.00

Statement of Work: Tasks/Deliverables Annoncé de travail: Tâches/Activités/Déliverables	Start/End Dates/Due Dates Debut/Fin/ Échéances
STATEMENT OF WORK:	

Signatures: **Signatures are required prior to the contractor commencing work. Les signatures sont exigants avant que l'entrepreneur commence le travail.**

Client Contract Authority	**Name/Nom:**	**Signature:**	**Date**	
RC Manager - Gestionnaire C	**Name/Nom:**	**Signature:**	**Date**	
Contractor Authorized Representative - Représentent de contracteur autorisé	**Name/Nom:**	**Signature:**	**Date**	
Procurement Authority - Autorité contractante	**Name/Nom**:	**Signature:**	**Date**	