

**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 complets, véridiques et exacts; et
4. si un contrat est attribué au soumissionnaire, ce dernier se conformera à toutes les modalités énoncées dans les clauses concernant 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
on – le	February 15, 2021/le 15 février 2021
Eastern Time (ET) Heure de l'Est (HE)	
F.O.B. - F.A.B.	
Plant-Usine: <input type="checkbox"/>	Destination: <input checked="" type="checkbox"/> Other-Autre: <input type="checkbox"/>
Address inquiries to – Adresser toute demande de renseignements à :	
Kristen Scott	
Area code and Telephone No. Code régional 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 adresse 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

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX.....	3
1.1 INTRODUCTION.....	3
1.2 SOMMAIRE	3
1.3 COMPTE RENDU.....	4
PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES.....	4
2.1 INSTRUCTIONS, CLAUSES ET CONDITIONS UNIFORMISÉES	4
2.2 PRÉSENTATION DES SOUMISSIONS	5
2.3 ANCIEN FONCTIONNAIRE	5
2.4 DEMANDES DE RENSEIGNEMENTS – EN PÉRIODE DE SOUMISSION.....	6
2.5 LOIS APPLICABLES	6
2.6 AMÉLIORATIONS APPORTÉES AU BESOIN PENDANT LA DEMANDE DE SOUMISSIONS.....	7
2.7 FONDEMENT DU TITRE DU CANADA SUR LES DROITS DE PROPRIÉTÉ INTELLECTUELLE.....	7
2.8 PROCESSUS DE CONTESTATION DES OFFRES ET MÉCANISMES DE RECOURS	7
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS	7
3.1 INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....	7
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION	9
4.1 PROCÉDURES D'ÉVALUATION.....	9
4.2 MÉTHODE DE SÉLECTION	9
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES.....	11
5.1 ATTESTATIONS EXIGÉES AVEC LA SOUMISSION	11
5.2 ATTESTATIONS PRÉALABLES À L'ATTRIBUTION DU CONTRAT ET RENSEIGNEMENTS SUPPLÉMENTAIRES ..11	
PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES	13
6.1 EXIGENCES RELATIVES À LA SÉCURITÉ.....	13
PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT	13
7.1 ÉNONCÉ DES TRAVAUX.....	13
7.2 CLAUSES ET CONDITIONS UNIFORMISÉES.....	14
7.3 EXIGENCES RELATIVES À LA SÉCURITÉ	14
7.4 DURÉE DU CONTRAT.....	15
7.5 RESPONSABLES.....	16
7.6 DIVULGATION PROACTIVE DE MARCHÉS CONCLUS AVEC D'ANCIENS FONCTIONNAIRES	17
7.7 PAIEMENT	17
7.7.5 INSTRUCTIONS RELATIVES À LA FACTURATION	18
7.8 ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES	18
7.9 LOIS APPLICABLES	18
7.10 ORDRE DE PRIORITÉ DES DOCUMENTS	18
7.11 ASSURANCES.....	19
ANNEXE « A »	20
ÉNONCÉ DES TRAVAUX	20
ANNEXE « B »	50
BASE DE PAIEMENT	50

ANNEXE « C »	54
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ	54
ANNEXE « D »	55
PROCESSUS D'ÉVALUATION	55
ANNEXE « E »	72
ANNEXE « F » DE LA PARTIE 3 DE LA DEMANDE DE SOUMISSIONS	78
INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE.....	78
ANNEXE « G » DE LA PARTIE 5 DE LA DEMANDE DE SOUMISSIONS	79
PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION.....	79
ANNEXE « H »	81
FORMULAIRE AUTORISATION DE TACHES	81

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

- | | |
|----------|---|
| Partie 1 | Renseignements généraux : renferme une description générale du besoin; |
| Partie 2 | Instructions à l'intention des soumissionnaires : renferme les instructions, clauses et conditions relatives à la demande de soumissions; |
| Partie 3 | Instructions pour la préparation des soumissions : donne aux soumissionnaires les instructions pour préparer leur soumission; |
| Partie 4 | Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection; |
| Partie 5 | Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir; |
| Partie 6 | Exigences relatives à la sécurité, exigences financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre; et |
| Partie 7 | Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent. |

Les annexes comprennent l'Énoncé des travaux, la Base de paiement, la Liste de vérification des exigences relatives à la sécurité, les instruments de paiement électronique, le Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, le formulaire Autorisation de tâches.

1.2 Sommaire

1.2.1 Transports Canada souhaite obtenir les services d'un expert-conseil ayant une expertise en gestion du trafic, en systèmes d'infrastructures essentielles, en évaluation et en vérification de la cybersécurité, en gestion des risques, en tests de pénétration, en consultation d'intervenants, en gestion de projets ainsi qu'en élaboration et en prestation de formations pour :

1. développer des outils servant à évaluer les profils de cybersécurité adaptés aux opérations des SGT et aux infrastructures connexes; aider les administrations routières à évaluer leurs niveaux actuel et cible de gestion des risques quant à la cybersécurité;
2. produire un document d'orientation sur la création ou l'amélioration d'un programme de gestion des risques en matière de cybersécurité pour les activités des SGT et les infrastructures connexes afin d'aider les administrations routières à atteindre et à maintenir leur niveau cible de gestion des risques quant à la cybersécurité;

-
3. fournir une formation et un soutien technique aux administrations routières pour qu'elles évaluent la cybersécurité au moyen des outils développés et établissent des programmes d'amélioration continue de la cybersécurité;
 4. offrir un soutien technique, une analyse et des conseils stratégiques, au besoin, concernant les nouveaux problèmes soulevés en matière de cybersécurité dans le secteur des transports;
 5. au besoin, effectuer des tests de pénétration sur les équipements et les réseaux du secteur des transports et analyser leurs vulnérabilités afin d'assurer la gestion des risques de cybersécurité émergents.
- 1.2.2 Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7, Clauses du contrat subséquent. Pour de plus amples renseignements sur les enquêtes de sécurité sur le personnel et les organismes, les soumissionnaires devraient consulter le site Web du [Programme de sécurité des contrats](http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html) de Travaux publics et Services gouvernementaux Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html>). »
- 1.2.3 Le Programme de contrats fédéraux pour l'équité en matière d'emploi s'applique au présent besoin; veuillez-vous référer à la Partie 5 – Attestations et renseignements supplémentaires, la Partie 7 – Clauses du contrat subséquent et l'annexe intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation.»

1.3 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le [Guide des clauses et conditions uniformisées d'achat](https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>) publié par Travaux publics et Services gouvernementaux Canada.

Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document [2003](#), (2020-05-28) Instructions uniformisées – biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Le paragraphe 5.4 du document [2003](#), Instructions uniformisées - biens ou services - besoins concurrentiels, est modifié comme suit :

Supprimer : 60 jours

Insérer : 120 jours

2.2 Présentation des soumissions

À moins d'indication contraire dans la demande de propositions, l'autorité contractuelle locale doit recevoir les soumissions identifiées en respect de la date, l'heure et l'endroit indiqués à la page -1- de la sollicitation. Si votre soumission est acheminée via courriel, le gouvernement du Canada ne se tient aucunement responsable de toute soumission reçue en retard à l'endroit désigné après la date et l'heure de clôture, et ce même si elle a été acheminée avant cette date.

Les soumissions doivent être envoyées par courriel à kristen.scott@tc.gc.ca

Référer à la Partie 3, section 3.1 « soumissions électronique »

2.3 Ancien fonctionnaire

Les contrats attribués à des anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à des anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu les renseignements requis, n'ont pas été fournis par le temps où l'évaluation des soumissions est complétée, le Canada informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Le défaut de se conformer à la demande du Canada et satisfaire à l'exigence dans le délai prescrit rendra la soumission non recevable.

Définition

Aux fins de cette clause, « ancien fonctionnaire » signifie tout ancien employé d'un ministère au sens de la [Loi sur la gestion des finances publiques](#), L.R., 1985, ch. F-11, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

- a. un individu;
- b. un individu qui s'est incorporé;
- c. une société de personnes constituée d'anciens fonctionnaires; ou
- d. une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« période du paiement forfaitaire » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'allocation de fin de services, qui se mesure de façon similaire.

« pension » signifie une pension ou une allocation annuelle versée en vertu de la [Loi sur la pension de la fonction publique](#) (LPFP), L.R., 1985, ch. P-36, et toute augmentation versée en vertu de la [Loi sur les prestations de retraite supplémentaires](#), L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la [Loi sur la pension de retraite des Forces canadiennes](#), L.R., 1985, ch. C-17, à la [Loi sur la continuation de la pension des services de défense](#), 1970, ch. D-3, à la [Loi sur la continuation des pensions de la Gendarmerie royale du Canada](#), 1970, ch. R-10, et à la Loi sur la pension de retraite de la Gendarmerie royale du Canada, L.R., 1985, ch. R-11, à la [Loi sur les allocations de retraite des parlementaires](#), L.R., 1985, ch. M-5, et à la partie de la pension versée conformément à la [Loi sur le Régime de pensions du Canada](#), L.R., 1985, ch. C-8.

Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension? **Oui () Non ()**

Si oui, le soumissionnaire doit fournir l'information suivante pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

- a. le nom de l'ancien fonctionnaire;
- b. la date de cessation d'emploi dans la fonction publique ou de la retraite.

En fournissant ces renseignements, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension, figure dans les rapports de divulgation proactive, sur les sites Web des ministères, conformément à l'[Avis sur la Politique des marchés : 2019-01](#) et aux [Lignes directrices sur la divulgation des marchés](#).

Directive sur le réaménagement des effectifs

Est-ce que le soumissionnaire est un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu de la Directive sur le réaménagement des effectifs? **Oui () Non ()**

Si oui, le soumissionnaire doit fournir l'information suivante :

- a. le nom de l'ancien fonctionnaire;
- b. les conditions de l'incitatif versé sous forme de paiement forfaitaire;
- c. la date de la cessation d'emploi;
- d. le montant du paiement forfaitaire;
- e. le taux de rémunération qui a servi au calcul du paiement forfaitaire;
- f. la période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines;
- g. nombre et montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

2.4 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins **7 (sept)** jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur Ontario, et les relations entre les parties seront déterminées par ces lois.

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.6 Améliorations apportées au besoin pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux contenus dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition qu'elles parviennent à l'autorité contractante au plus tard 25 jours avant la date de clôture de la demande de soumissions. Le Canada aura le droit d'accepter ou de rejeter n'importe quelle ou la totalité des suggestions proposées.

2.7 Fondement du titre du Canada sur les droits de propriété intellectuelle

Le ministère des transports a déterminé que tout droit de propriété intellectuelle découlant de l'exécution des travaux prévus par le contrat subséquent appartiendra au Canada, pour les motifs suivants, tel que défini dans la [Politique sur les droits de propriété intellectuelle issus de marchés conclus avec l'État](#) : Lorsque le marché conclu avec l'État ou les produits à livrer aux termes de celui-ci visent surtout 4.1 à obtenir des connaissances et des renseignements qui seront diffusés au public.

2.8 Processus de contestation des offres et mécanismes de recours

- (a) Les fournisseurs potentiels ont accès à plusieurs mécanismes pour contester des aspects du processus d'approvisionnement jusqu'à l'attribution du marché, inclusivement.
- (b) Le Canada invite les fournisseurs à porter d'abord leurs préoccupations à l'attention de l'autorité contractante. Le site Web du Canada [Achats et ventes](#), sous le titre « [Processus de contestation des soumissions et mécanismes de recours](#) », fournit de l'information sur les organismes de traitement des plaintes possibles, notamment :
 - Bureau de l'ombudsman de l'approvisionnement (BOA)
 - Tribunal canadien du commerce extérieur (TCCE)
- (c) Les fournisseurs devraient savoir que des **délais stricts** sont fixés pour le dépôt des plaintes et qu'ils varient en fonction de l'organisation concernée. Les fournisseurs devraient donc agir rapidement s'ils souhaitent contester un aspect du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

Le soumissionnaire doit soumettre sa soumission par voie électronique. Le Canada demande que la soumission soit présentée en sections distinctes, comme suit :

Section I : Soumission technique : (Une (1) copie électronique, soumise par courriel)
Section II : Soumission financière : (Une (1) copie électronique, soumise par courriel)
Section III : Attestations non inclus dans la soumission technique : (Une (1) copie électronique, soumise par courriel)

Les soumissions doivent être envoyées par courriel à : kristen.scott@tc.gc.ca

Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de la soumission.

Section I : Soumission technique

Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires devraient démontrer leur capacité« et décrire l'approche qu'ils prendront » de façon complète, concise et claire pour effectuer les travaux.

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

Section II : Soumission financière

Les soumissionnaires doivent présenter leur soumission financière en conformité avec « le barème de prix à l'annexe « E ».

3.1.1 Soumission Électronique

Les soumissionnaires intéressés sont invités à faire parvenir leur soumission, par voie électronique, à: kristen.scott@tc.gc.ca

Tout courriel excédant cinq mégaoctets (5MB), ou contenant d'autres items, tels que des macros intégrées et/ou des liens internet, pourrait être bloqué par le système de courrier électronique et/ou le pare-feu de Transports Canada, sans que cela ne génère un avis à l'intention du soumissionnaire ou de l'autorité contractuelle. Les soumissions plus volumineuses peuvent être acheminées par l'entremise de plusieurs courriels. L'autorité contractuelle confirmera la réception de ces documents. Le soumissionnaire a la responsabilité de s'assurer que l'autorité contractuelle a reçu sa soumission dans son intégralité.

3.1.2 Paiement électronique de factures – soumission

Si vous êtes disposés à accepter le paiement de factures au moyen d'instruments de paiement électronique, compléter l'annexe « F » Instruments de paiement électronique, afin d'identifier lesquels sont acceptés.

Si l'annexe « F » Instruments de paiement électronique n'a pas été complétée, il sera alors convenu que le paiement de factures au moyen d'instruments de paiement électronique ne sera pas accepté.

L'acceptation des instruments de paiement électronique ne sera pas considérée comme un critère d'évaluation.

Section III : Attestations

Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5.

Section IV : Renseignements supplémentaires

3.1.3 Installations ou locaux proposés par le soumissionnaire nécessitant des mesures de sauvegarde

3.1.3.1 Tel qu'indiqué à la Partie 6 Exigences relatives à la sécurité, le soumissionnaire doit fournir l'adresse complète de ses installations ou de ses locaux et celles des individus proposés, pour lesquelles des mesures de sauvegarde sont nécessaires à la réalisation des travaux :

N° civique / nom de la rue, unité / N° de bureau / d'appartement
Ville, province, territoire / État
Code postal / code zip
Pays

3.1.3.2 L'agent de sécurité d'entreprise doit s'assurer, par l'entremise du [Programme de sécurité des contrats](#) que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé, tel que décrit à la Partie 6 – Exigences relatives à la sécurité, exigences financières et autres exigences.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

- a) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation techniques et financiers.
- b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

4.1.1 Évaluation technique

Les critères techniques obligatoires et les critères techniques cotés sont inclus dans l'annexe « D ».

4.1.2 Évaluation financière

4.1.2.1 Critères financiers obligatoires

Le prix de la soumission sera évalué en dollars canadiens, excluant les taxes applicables, FAB destination, incluant les droits de douane et les taxes d'accise canadiens.

4.2 Méthode de sélection

4.2.1 [A0027T](#) Note combinée la plus haute sur le plan du mérite technique et du prix

Pour être jugée recevable, une soumission doit :

- I. satisfaire à toutes les exigences de la demande de soumissions;
- II. satisfaire à tous les critères obligatoires;
- III. obtenir au moins 65 points pour l'ensemble des critères d'évaluation technique faisant l'objet de la cotation;

IV. proposer un prix total pour les tâches 5.1 à 5.5 et des tarifs journaliers pour les tâches 5.6.1, 5.6.2 et 5.6.3.

Remarque : les tarifs journaliers proposés pour les tâches 5.6.1, 5.6.2 et 5.6.3 peuvent être propres aux exigences prévues pour l'expérience et la qualification des ressources. Les soumissionnaires doivent fournir un tarif journalier qui couvre toute combinaison de ressources nécessaires au travail pour chaque tâche optionnelle.

1. L'évaluation est effectuée sur un barème de 100 points.
2. Les offres qui ne répondent pas aux critères 1 i à iv seront déclarées irrecevables.
3. La sélection sera faite en fonction de la meilleure note combinée pour le mérite technique et le prix. Le ratio sera de 70 % pour le mérite technique et de 30 % pour le prix.
4. Afin de calculer la note pour le mérite technique, la note technique globale de chaque soumission recevable sera déterminée comme suit : le nombre total de points obtenus divisé par le nombre maximum de points pouvant être accordés, multiplié par le rapport de 70 %.
5. Afin de calculer la note pour le prix, chaque soumission recevable sera évaluée proportionnellement par rapport au prix évalué le plus bas pour chaque groupe de tâches conformément au tableau ci-dessous et selon le ratio de 30 %.

Tâches	Tarif journalier total de la soumission	Prix évalué total	Pondération	Nombre maximum de points
5.1 à 5.5	S. O.	Prix total fixe évalué dans la table A de la proposition de coût	50 %	15
5.6 [(5.6.1 + 5.6.2 + 5.6.3) / 3]	Tarif journalier moyen dans la table B de la Proposition de coût	S. O.	50 %	15
Total			100 %	30

6. Pour chaque soumission recevable, la note du mérite technique et la note du prix seront additionnées de manière à donner la note combinée.
7. La soumission choisie ne sera pas nécessairement la soumission recevable ayant obtenu la cote la plus élevée pour le mérite technique ni celle ayant le prix évalué le plus bas. La soumission recevable assortie de la note combinée la plus élevée pour le mérite technique et le prix sera recommandée pour l'attribution d'un contrat.

Remarques :

* TC peut décider de mettre fin à l'évaluation dès le premier constat de non-respect.

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fautive, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations exigées avec la soumission

Les soumissionnaires doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Dispositions relatives à l'intégrité - déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des instructions uniformisées, tous les soumissionnaires doivent présenter avec leur soumission, **s'il y a lieu**, le formulaire de déclaration d'intégrité disponible sur le site Web [Intégrité – Formulaire de déclaration](http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html>), afin que leur soumission ne soit pas rejetée du processus d'approvisionnement.

5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la soumission mais ils peuvent être fournis plus tard. Si l'une de ces attestations ou renseignements supplémentaires ne sont pas remplis et fournis tel que demandé, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations ou les renseignements supplémentaires énumérés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.2.1 Dispositions relatives à l'intégrité – documentation exigée

Conformément à l'article intitulé Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier de la [Politique d'inadmissibilité et de suspension](http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html>), le soumissionnaire doit présenter la documentation exigée, s'il y a lieu, afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

5.2.2 Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation de soumission

En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page du site Web [d'Emploi et Développement social](#)

[Canada \(EDSC\) – Travail \(https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html#s4\)](https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html#s4).

Le Canada aura le droit de déclarer une soumission non recevable si le soumissionnaire, ou tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure dans la liste des « soumissionnaires à admissibilité limitée du PCF » au moment de l'attribution du contrat.

Le Canada aura aussi le droit de résilier le contrat pour manquement si l'entrepreneur, ou tout membre de la coentreprise si l'entrepreneur est une coentreprise, figure dans la liste des « soumissionnaires à admissibilité limitée du PCF » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante l'annexe intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation remplie avant l'attribution du contrat. Si le soumissionnaire est une coentreprise, il doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation remplie pour chaque membre de la coentreprise.

5.2.3 Attestations additionnelles préalables à l'attribution du contrat

5.2.3.1 Statut et disponibilité du personnel

Le soumissionnaire atteste que, s'il obtient le contrat découlant de la demande de soumissions, chaque individu proposé dans sa soumission sera disponible pour exécuter les travaux, tel qu'exigé par les représentants du Canada, au moment indiqué dans la demande de soumissions ou convenue avec ce dernier. Si pour des raisons hors de son contrôle, le soumissionnaire est incapable de fournir les services d'un individu identifié dans sa soumission, le soumissionnaire peut proposer un remplaçant avec des qualités et une expérience similaires. Le soumissionnaire doit aviser l'autorité contractante de la raison pour le remplacement et fournir le nom, les qualités et l'expérience du remplaçant proposé. Pour les fins de cette clause, seule les raisons suivantes seront considérées comme étant hors du contrôle du soumissionnaire : la mort, la maladie, le congé de maternité et parental, la retraite, la démission, le congédiement justifié ou la résiliation par manquement d'une entente.

Si le soumissionnaire a proposé un individu qui n'est pas un employé du soumissionnaire, le soumissionnaire atteste qu'il a la permission de l'individu d'offrir ses services pour l'exécution des travaux et de soumettre son curriculum vitae au Canada. Le soumissionnaire doit, sur demande de l'autorité contractante, fournir une confirmation écrite, signée par l'individu, de la permission donnée au soumissionnaire ainsi que de sa disponibilité. Le défaut de répondre à la demande pourrait avoir pour conséquence que la soumission soit déclarée non recevable.

5.2.3.2 Études et expérience

Le soumissionnaire atteste qu'il a vérifié tous les renseignements fournis dans les curriculum vitae et les documents à l'appui présentés avec sa soumission, plus particulièrement les renseignements relatifs aux études, aux réalisations, à l'expérience et aux antécédents professionnels, et que ceux-ci sont exacts. En outre, le soumissionnaire garantit que chaque individu qu'il a proposé est en mesure d'exécuter les travaux prévus dans le contrat éventuel.

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Exigences relatives à la sécurité

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :
 - a) le soumissionnaire doit détenir une attestation de sécurité d'organisme valable tel qu'indiqué à la Partie 7 – Clauses du contrat subséquent;
 - b) les individus proposés par le soumissionnaire et qui doivent avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé doivent posséder une attestation de sécurité tel qu'indiqué à la Partie 7 – Clauses du contrat subséquent;
 - c) le soumissionnaire doit fournir le nom de tous les individus qui devront avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé;
 - d) le lieu proposé par le soumissionnaire pour la réalisation des travaux et la sauvegarde des documents doit satisfaire aux exigences relatives à la sécurité précisées à la Partie 7– Clauses du contrat subséquent;
 - e) le soumissionnaire doit fournir l'adresse des lieux proposés pour la réalisation des travaux et la sauvegarde des documents, tel qu'indiqué à la Partie 3 – section IV Renseignements supplémentaires.
2. On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir la cote de sécurité requise, demeure à l'entière discrétion de l'autorité contractante.
3. Pour de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le site Web du [Programme de sécurité des contrats](http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html) de Travaux publics et Services gouvernementaux Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html>).

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

Les clauses et conditions suivantes s'appliquent à tout contrat subséquent découlant de la demande de soumissions et en font partie intégrante.

7.1 Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux qui se trouve à l'annexe « A ».

7.1.2 Autorisation de tâches

La totalité ou une partie des travaux du contrat seront réalisés sur demande, au moyen d'une autorisation de tâches. Les travaux décrits dans l'autorisation de tâches doivent être conformes à la portée du contrat.

7.1.2.1 Processus d'autorisation de tâches

1. Le chargé de projet fournira à l'entrepreneur une description des tâches au moyen du « Formulaire d'autorisation des tâches » de l'annexe « H ».
2. L'AT comprendra les détails des activités à exécuter, une description des produits à livrer et un calendrier indiquant les dates d'achèvement des activités principales ou les dates de livraison des produits livrables. L'AT comprendra également les bases et les méthodes de paiement applicables, comme le précise le contrat.
3. Dans les cinq (5) jours civils suivant la réception de l'AT, l'entrepreneur doit fournir au chargé de projet le coût total estimatif proposé pour l'exécution des tâches et une ventilation de ce coût, établie conformément à la Base de paiement du contrat.
4. L'entrepreneur ne doit pas commencer les travaux avant la réception de l'AT autorisée par le chargé de projet. L'entrepreneur reconnaît qu'avant la réception d'une AT le travail effectué sera à ses propres risques.

7.1.2.2 Limite d'autorisation de tâches

L'obligation du Canada à l'égard de la portion des travaux qui est réalisée en vertu du contrat au moyen d'autorisations de tâches est limitée au montant total des tâches effectivement réalisées par l'entrepreneur.

7.2 Clauses et conditions uniformisées

Toutes les clauses et conditions identifiées dans le contrat par un numéro, une date et un titre sont reproduites dans le [Guide des clauses et conditions uniformisées d'achat](https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>) publié par Travaux publics et Services gouvernementaux Canada.

7.2.1 Conditions générales

[2035](#) (2020-05-28), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

7.2.2 Conditions générales supplémentaires

[4007](#) (2010-08-16) Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux, s'appliquent au contrat et en font partie intégrante.

7.3 Exigences relatives à la sécurité

7.3.1 Les exigences relatives à la sécurité suivantes (LVERS et clauses connexes, tel que prévu par le Programme de sécurité des contrats) s'appliquent et font partie intégrante du contrat.

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de VOD en vigueur, ainsi qu'une cote de protection des

documents approuvée au niveau **protégé B**, délivrées par le Programme de Sécurité des Contrats (PSC) du Secteur de la SSI de SPAC

2. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens protégés/classifiés, ou à des établissements de travail dont l'accès est réglementé, doivent tous détenir une cote de sécurité du personnel valable au niveau fiabilité ou secret tel que requis, délivrée ou approuvée par le PSC/SSI/SPAC
3. L'entrepreneur ou l'offrant ne doit pas emporter de renseignements protégés/classifiés hors des établissements de travail visés; et l'entrepreneur ou l'offrant doit s'assurer que son personnel est au courant de cette restriction et qu'il l'a respecte
4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité ne doivent pas être attribués sans l'autorisation écrite préalable du PSC/SSI/SPAC
5. L'entrepreneur ne doit pas utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau protégés/classifiés tant que le PSC/SSI/SPAC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées jusqu'au niveau **protégé B**.
6. L'entrepreneur ou l'offrant doit respecter les dispositions :
 1. de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe C
 2. du Manuel de la sécurité industrielle (dernière édition)

7.3.2 Installations ou locaux de l'entrepreneur nécessitant des mesures de sauvegarde

- 7.3.2.1 Lorsque des mesures de sauvegarde sont nécessaires pour réaliser les travaux, l'entrepreneur doit diligemment tenir à jour les renseignements relatifs à ses installations ou à ses locaux, et ceux des individus proposés pour les adresses suivantes :

Numéro civique / nom de la rue, unité / N° de bureau / d'appartement
Ville, province, territoire / État
Code postal / code zip
Pays

- 7.3.2.2 L'agent de sécurité d'entreprise doit s'assurer, par l'entremise du [Programme de sécurité des contrats](#) que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé.

7.4 Durée du contrat

7.4.1 Période du contrat

La période du contrat est à partir de la date du contrat jusqu'au 31 mars 2024 inclusivement.

7.4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable d'acquérir les biens, les services ou les deux, qui sont décrits à section 5.6 d'énoncé des travaux selon les mêmes conditions et aux prix et(ou) aux taux établis dans le contrat. Cette option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur avant la date d'expiration du contrat.

7.5 Responsables

7.5.1 Autorité contractante

L'autorité contractante pour le contrat est:

Nom : Kristen Scott
Titre : Spécialiste des contrats
Transports Canada
95 rue Foundry
Moncton, NB E1C 5H7
Téléphone : 506-377-2564
Courriel : kristen.scott@tc.gc.ca

L'autorité contractante est responsable de la gestion du contrat, et toute modification doit être autorisée par écrit par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou des travaux qui n'y sont pas prévus, suite à des demandes ou instructions verbales ou écrites de toute personne autre que l'autorité contractante.

7.5.2 Chargé de projet

Le chargé de projet pour le contrat est : (sera fourni lors de l'attribution du contrat)

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____

Téléphone : ____ - ____ - _____
Télécopieur : ____ - ____ - _____
Courriel : _____

Le chargé de projet représente le ministère ou l'organisme pour lequel les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le chargé de projet; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. De tels changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

7.5.3 Représentant de l'entrepreneur (À déterminer)

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : ____ - ____ - _____
Courriel : _____

7.6 Divulgence proactive de marchés conclus avec d'anciens fonctionnaires

En fournissant de l'information sur son statut en tant qu'ancien fonctionnaire touchant une pension en vertu de la [Loi sur la pension de la fonction publique](#) (LPFP), l'entrepreneur a accepté que cette information soit publiée sur les sites Web des ministères, dans le cadre des rapports de divulgation proactive des marchés, et ce, conformément à l'[Avis sur la Politique des marchés : 2019-01](#) du Secrétariat du Conseil du Trésor du Canada.

7.7 Paiement

7.7.1 Base de paiement

Pour les travaux décrits dans L'énoncé des travaux à l'annexe « A » :

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera selon un montant total fixe de de \$ _____ (montant à insérer lors de l'attribution du contrat)

Les droits de douane sont inclus et les taxes applicables sont en sus.

L'entrepreneur sera payé pour les travaux spécifiés dans l'autorisation de tâches autorisée, conformément à la base de paiement à l'annexe «B».

Pour la portion des travaux faisant l'objet d'un prix ferme seulement, le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

7.7.2 Paiements d'étape

Le Canada effectuera les paiements d'étape conformément au calendrier des étapes détaillé dans le contrat et les dispositions de paiement du contrat si :

- a. une demande de paiement exacte et complète et tout autre document exigé par le contrat ont été présentés conformément aux instructions relatives à la facturation fournies dans le contrat;
- b. tous les travaux associés à l'étape et, selon le cas, tout bien livrable exigé ont été complétés et acceptés par le Canada.

7.7.3 Paiement électronique de factures – contrat

L'entrepreneur accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

- a. Carte d'achat Visa ;
- b. Carte d'achat MasterCard ;
- c. Dépôt direct (national et international) ;
- d. Échange de données informatisées (EDI) ;
- e. Virement télégraphique (international seulement) ;

7.7.4 Vérification du temps

Le temps facturé et l'exactitude du système d'enregistrement du temps de l'entrepreneur peuvent faire l'objet d'une vérification par le Canada, avant ou après que l'entrepreneur ait été payé. Si la vérification est effectuée après le paiement, l'entrepreneur devra rembourser, à la demande du Canada, tout paiement en trop.

7.7.5 Instructions relatives à la facturation

L'entrepreneur doit soumettre les factures conformément à l'article intitulé « Présentation des factures » des conditions générales. Les factures ne doivent pas être soumises avant que les travaux identifiés dans la facture soient complétés. Chaque facture doit être appuyée par:

- a. une copie des feuilles de temps pour corroborer le temps de travail réclamé;
- b. une copie du document de sortie et de tout autre document tel qu'il est spécifié au contrat;
- c. la description et valeur du jalon réclamé tel que détaillé dans l'énoncé des travaux.

7.8 Attestations et renseignements supplémentaires

7.8.1 Conformité

À moins d'indication contraire, le respect continu des attestations fournies par l'entrepreneur avec sa soumission ou préalablement à l'attribution du contrat, ainsi que la coopération constante quant aux renseignements supplémentaires, sont des conditions du contrat et leur non-respect constituera un manquement de la part de l'entrepreneur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

7.8.2 Programme de contrats fédéraux pour l'équité en matière d'emploi - Manquement de la part de l'entrepreneur

Lorsqu'un Accord pour la mise en œuvre de l'équité en matière d'emploi a été conclu avec Emploi et Développement social Canada (EDSC) – Travail, l'entrepreneur reconnaît et s'engage, à ce que cet accord demeure valide pendant toute la durée du contrat. Si l'Accord pour la mise en œuvre de l'équité en matière d'emploi devient invalide, le nom de l'entrepreneur sera ajouté à la liste des « [soumissionnaires à admissibilité limitée du PCF](#) ». L'imposition d'une telle sanction par EDSC fera en sorte que l'entrepreneur sera considéré non conforme aux modalités du contrat.

7.9 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur Ontario et les relations entre les parties seront déterminées par ces lois.

7.10 Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.

- a) les articles de la convention;
- b) les conditions générales supplémentaires [4007](#) (2010-08-16) Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux,
- c) les conditions générales - [2035](#) (2020-05-28), Conditions générales - besoins plus complexes de services;

-
- d) l'Annexe « A », Énoncé des travaux;
 - e) l'Annexe « B », Base de paiement;
 - f) l'Annexe « C », Liste de vérification des exigences relatives à la sécurité;
 - h) les autorisations de tâches signées;
 - i) la soumission de l'entrepreneur datée du _____, (*inscrire la date de la soumission*)

7.11 Assurances

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du contrat et pour se conformer aux lois applicables. Toute assurance souscrite ou maintenue par l'entrepreneur est à sa charge ainsi que pour son bénéfice et sa protection. Elle ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat, ni ne la diminue.

ANNEXE « A »

ÉNONCÉ DES TRAVAUX

Améliorer la préparation à la cybersécurité des propriétaires ou des exploitants des infrastructures routières du Canada en vue d'une meilleure connectivité et automatisation

1 Introduction

Transports Canada souhaite obtenir les services d'un expert-conseil pour l'élaboration d'outils, de documents d'orientation et de programmes de formation et pour apporter un soutien technique aux administrations routières (p. ex. les provinces, les territoires et les municipalités), qui ont à évaluer et à améliorer l'état de la cybersécurité de leurs systèmes de gestion du trafic (SGT), y compris les systèmes de transport intelligents (STI). Les produits du travail seront conçus pour aider les administrations routières à gérer les risques actuels et à se préparer à intégrer en toute sécurité de nouvelles technologies ainsi qu'une meilleure connectivité et automatisation (p. ex. des véhicules connectés et automatisés) dans leurs réseaux de transport.

2 Contexte

Au Canada, le transport routier est une responsabilité que se partagent les gouvernements fédéral, provinciaux et territoriaux et les administrations locales (comme les municipalités). Les infrastructures de transport sont généralement détenues et exploitées par les gouvernements provinciaux et territoriaux ou les administrations locales.

Le mandat de Transports Canada est de promouvoir un réseau de transport sûr et sécuritaire, respectueux de l'environnement, efficace, et novateur par l'élaboration et la supervision des politiques et des programmes de transport du gouvernement du Canada. Transports Canada mène une série d'activités afin de perfectionner les connaissances scientifiques et de développer les technologies requises pour contribuer à la mission du Ministère et favoriser l'innovation dans le secteur canadien des transports.

En 2017, Transports Canada a lancé le Programme de promotion de la connectivité et l'automatisation du système de transports (PCAST) pour aider les provinces et les territoires du Canada à se préparer à une série de problèmes techniques et de questions réglementaires et stratégiques qui découleront de l'arrivée des véhicules connectés et automatisés (VCA). Le programme appuie la recherche, les essais, l'élaboration de codes, de normes et de documents d'orientation, ainsi que les activités de renforcement des capacités et de partage des connaissances. Un des volets privilégiés du programme est le renforcement de la cybersécurité des systèmes d'infrastructures intelligentes (SII).

Les SII combinent les technologies de l'information (TI) (p. ex. les logiciels de surveillance de la circulation, les réseaux ministériels et les systèmes de paiement) et les technologies opérationnelles (TO) (p. ex. les contrôleurs de feux de circulation, les panneaux à messages variables et les unités de bord de route pour les VCA) afin d'améliorer la sécurité et l'efficacité du transport routier.

Certaines de ces technologies (p. ex. la régulation de bretelles d'accès et le système de commande prioritaire des feux de circulation) existent depuis des dizaines d'années. Des technologies plus récentes comme la détection Bluetooth, la vidéo haute définition, les contrôleurs de signaux avancés et les équipements de communication routière des VCA offrent des avantages supplémentaires en matière de sécurité et d'efficacité, mais augmentent à la fois la connectivité et les risques de cybermenaces.

Bien que certaines technologies récentes de STI aient été conçues en tenant compte des principes de cybersécurité, ce n'est pas le cas pour un bon nombre d'entre elles. En plus des vulnérabilités que peut présenter le matériel mobile, l'intégration de nouveaux et d'anciens systèmes entraîne souvent d'autres vulnérabilités aux cyberattaques. L'élargissement de la surface d'attaque, la limite entre les TI et les TO, ainsi que les risques que présente l'intégration des systèmes en sont les causes. Les anciens systèmes étaient souvent fermés, étaient électromécaniques plutôt qu'informatisés et n'étaient pas accessibles par une connexion sans fil. De plus, les problèmes de sécurité à résoudre étaient plus physiques que cybernétiques. Bon nombre de ces anciens systèmes ont été convertis pour être accessibles par Internet, par exemple pour faciliter les activités et la maintenance, rendant ainsi ces systèmes vulnérables aux

cyberattaques à distance. Enfin, on s'attend à ce que l'Internet des objets, le déploiement des VCA et l'infrastructure numérique de soutien apportent de nouvelles connexions et interfaces présentant des risques à gérer de manière appropriée.

Ce projet vise à fournir aux propriétaires et aux gestionnaires d'infrastructures ainsi qu'aux agences de transport (collectivement « administrations routières¹ ») un ensemble d'outils d'évaluation des risques en matière de cybersécurité, des documents d'orientation, des formations et un soutien technique personnalisé à leurs besoins opérationnels. Plus précisément, le projet orientera les administrations routières pour qu'elles puissent développer ou améliorer un programme de cybersécurité existant, conformément au cadre du National Institute of Standards and Technology (NIST) pour l'amélioration de la cybersécurité des infrastructures essentielles (point 3.2, étapes 1 à 7), ainsi que des outils qui contribueront à la création d'un profil actuel (étape 3) et d'un profil cible (étape 5).

Ce projet devrait exploiter et compléter les recherches, les normes, l'orientation et les outils existants en matière de cybersécurité, qui ont été élaborés pour le transport et d'autres secteurs d'infrastructures essentielles. Les annexes suivantes appuient le présent énoncé des travaux :

1. Annexe A – Définition des termes techniques utilisés dans l'énoncé des travaux
2. Annexe B – Liste des ressources techniques existantes
3. Annexe C – Résumé des travaux connexes

3 Objectifs

Transports Canada souhaite obtenir les services d'un expert-conseil ayant une expertise en gestion du trafic, en systèmes d'infrastructures essentielles, en évaluation et en vérification de la cybersécurité, en gestion des risques, en tests de pénétration, en consultation d'intervenants, en gestion de projets ainsi qu'en élaboration et en prestation de formations pour :

6. développer des outils servant à évaluer les profils de cybersécurité adaptés aux opérations des SGT et aux infrastructures connexes; aider les administrations routières à évaluer leurs niveaux actuel et cible de gestion des risques quant à la cybersécurité;
7. produire un document d'orientation sur la création ou l'amélioration d'un programme de gestion des risques en matière de cybersécurité pour les activités des SGT et les infrastructures connexes afin d'aider les administrations routières à atteindre et à maintenir leur niveau cible de gestion des risques quant à la cybersécurité;
8. fournir une formation et un soutien technique aux administrations routières pour qu'elles évaluent la cybersécurité au moyen des outils développés et établissent des programmes d'amélioration continue de la cybersécurité;
9. offrir un soutien technique, une analyse et des conseils stratégiques, au besoin, concernant les nouveaux problèmes soulevés en matière de cybersécurité dans le secteur des transports;
10. au besoin, effectuer des tests de pénétration sur les équipements et les réseaux du secteur des transports et analyser leurs vulnérabilités afin d'assurer la gestion des risques de cybersécurité émergents.

¹ Aux fins du présent énoncé des travaux, ce terme désigne les organisations provinciales, territoriales et municipales qui sont responsables de la gestion des infrastructures routières, du trafic et des services de transport en commun.

4 Portée

4.1 Activités couvertes par la portée

Les activités suivantes s'appliquent à la réalisation des tâches et aux livrables, comme le présentent les points 5 et 6.

- 4.1.1 Organisation et tenue d'une réunion de lancement au début du projet.**
- 4.1.2 Élaboration des plans du projet pour la planification et l'accomplissement des tâches et des livrables et pour l'affectation des ressources.**
- 4.1.3 Examen des rapports et des normes techniques, des lois, des spécifications et des manuels concernant l'équipement, des procédures d'essai, et des documents techniques.**
- 4.1.4 En coordination avec Transports Canada, organisation des séances de consultation avec les parties prenantes, élaboration des ordres du jour, animation, recueil des commentaires des participants et présentation des résultats du projet lors des séances.**
- 4.1.5 Transmission des rapports de synthèse découlant des séances de consultation.**
- 4.1.6 Animation et présentation lors des réunions et des séances d'information avec les gestionnaires et les employés du gouvernement du Canada afin de communiquer davantage les renseignements requis.**
- 4.1.7 Organisation (fixer le lieu, fournir les documents de formation et procéder à l'accueil) et prestation des formations.**
- 4.1.8 Élaboration des grandes lignes du rapport, production des versions provisoires, intermédiaires et finales des rapports ou des livrables.**
- 4.1.9 Réponse aux commentaires reçus sur les livrables du projet (plans du projet; rapports provisoires, intermédiaires et finaux) de la part de Transports Canada et des parties prenantes pertinentes, intégration de ces commentaires et transmission des rapports de résolution.**
- 4.1.10 Création de graphiques et de schémas, s'il y a lieu, à intégrer dans les rapports, les présentations et les documents de formation.**
- 4.1.11 Création de questionnaires et d'outils basés sur les logiciels, notamment la rédaction et la maintenance du code source (selon le format de l'outil qu'aura déterminé le responsable technique).**
- 4.1.12 Soutien technique offert sur place aux parties prenantes pour la mise en place et l'exécution des évaluations, l'élaboration des programmes d'amélioration de la cybersécurité, et l'évaluation ou l'essai des vulnérabilités du système et des stratégies d'atténuation des risques.**
- 4.1.13 Tests de pénétration effectués sur l'équipement et les réseaux de transport au moyen du matériel, des logiciels et des autres outils fournis par l'entrepreneur, dans un environnement sécurisé.**

Remarque : L'entrepreneur est censé avoir accès, directement ou par la sous-traitance, à une gamme d'outils pour réaliser les tests de pénétration et à du personnel pouvant obtenir du gouvernement du Canada une cote de sécurité de niveau SECRET, qui sera nécessaire pour effectuer l'analyse.

Les achats de l'équipement à tester seront remboursés conformément au point 18.5, après leur préautorisation par le ministère des Transports, et sont exclus du prix concurrentiel de la soumission.

4.1.14 Achat, aux frais de l'entrepreneur, des normes techniques nécessaires à l'exécution de l'une ou l'autre des tâches.

4.1.15 Temps des déplacements du personnel de l'entrepreneur.

Remarque : Les coûts liés aux déplacements (vols, taxis, hébergement, repas), sur présentation d'un reçu, seront remboursés conformément au point 11, après leur préautorisation par le ministère des Transports, et sont exclus du prix concurrentiel de la soumission.

4.2 Activités non couvertes par la portée

4.2.1 Traduction des livrables, de l'anglais vers le français (Transports Canada s'occupe de prévoir la traduction, le cas échéant).

4.2.2 Interprétation simultanée pendant les formations et les séances de consultation (Transports Canada s'occupe de prévoir l'interprétation, le cas échéant).

5 Tâches et exigences

5.1 Plan du projet

Après la réunion de lancement, et à toutes les semaines (ou selon une fréquence fixée avec le responsable technique), faire une mise à jour du plan du projet présentant les progrès hebdomadaires des tâches et des livrables ainsi que la répartition des ressources. Le format du plan du projet (p. ex. MS Project ou Excel) sera déterminé en concertation avec le responsable technique.

5.2 Revue de la littérature, abécédaire de la cybersécurité dans les transports routiers, et documents d'information

5.2.1 Examiner les outils d'évaluation de la cybersécurité et les cadres de gestion des risques qui s'appliquent aux secteurs des transports et des infrastructures essentielles. La revue en question doit traiter des documents figurant à l'annexe A – Références techniques.

Remarque : Aucun livrable officiel n'est associé à la tâche 5.2.1. Bien qu'un rapport sommaire ne soit pas requis, l'entrepreneur est censé connaître ces ressources pour pouvoir effectuer les autres tâches mentionnées dans cette section.

5.2.2 Élaborer un plan et une approche en vue de créer les outils de la tâche 5.2. Le plan doit préciser comment les outils de cybersécurité pour les infrastructures essentielles et les cadres de gestion des risques seront adaptés aux SGT et aux infrastructures connexes. Le plan doit également expliquer les options relatives à la logique d'évaluation des outils en matière de cybersécurité.

5.2.3 Élaborer un abécédaire de la cybersécurité dans les transports routiers (environ 15 pages), adapté au personnel et aux gestionnaires de divers postes de l'organisation (opérations, finances, RH, politique, etc.). Le document doit comprendre un glossaire des termes relatifs à la cybersécurité et expliquer des questions primordiales, telles que :

- a) les effets des véhicules connectés et automatisés sur la cybersécurité des SGT, et inversement;
- b) les similitudes et les différences entre la cybersécurité des TI et celle des TO;
- c) la relation entre la sécurité numérique et physique;
- d) les rôles, les responsabilités et les mandats de l'industrie et des différents ordres de gouvernement;
- e) l'incidence de la cybersécurité des TO sur les différents domaines fonctionnels d'une organisation (opérations, finances, RH, politiques, TI, etc.);
- f) des exemples publiquement disponibles d'atteintes à la cybersécurité ou d'incidents causés par une cybersécurité insuffisante ou des vulnérabilités dans le secteur des infrastructures du transport routier;
- g) les coûts et les risques découlant d'une mauvaise gestion des risques liés à la cybersécurité;
- h) l'importance d'élaborer des politiques de cybersécurité au sein d'une organisation et de guider la méthode utilisée pour y arriver;
- i) le contexte de base des menaces des SGT et des VCA;
- j) l'utilisation d'une approche d'ingénierie des systèmes aux fins d'architecture, de conception, de déploiement et de maintenance de l'infrastructure et des produits des SGT (c.-à-d. NIST 800-160 ou ISO 15288).

5.2.4 Avec la collaboration du responsable technique, élaboration d'une liste de vingt (20) questions fréquentes (FAQ) et de leurs réponses, portant sur la cybersécurité des infrastructures du transport routier.

5.2.5 Produire un document d'information (environ deux pages) et une présentation (environ 20 diapositives) basés sur le guide (5.2.3) et adaptés aux cadres supérieurs et aux décideurs. L'objectif de ces documents est d'aider les décideurs à comprendre la nécessité d'investir dans la planification, les ressources et la formation en matière de cybersécurité dans leurs organisations. La présentation comprendrait certains termes et concepts de base de la cybersécurité des TI et des TO, des considérations clés (stratégiques, organisationnelles, RH, financières) et d'autres renseignements nécessaires pour sensibiliser les participants à la cybersécurité.

5.2.6 Organiser au plus six (6) séances de formation virtuelle (d'environ 1 heure chacune, y compris la période de questions) destinée aux cadres supérieurs et aux décideurs, en utilisant les documents préparés à la tâche 5.2.5. Peaufiner le document d'information, la présentation et la FAQ selon les besoins.

5.2.7 Concevoir un webinaire enregistré de façon autonome reposant sur la formation virtuelle, pour accompagner le document d'information et la présentation.**5.3 Boîte à outils pour l'auto-évaluation de la cybersécurité adaptée aux opérations des SGT et aux infrastructures connexes**

À cette tâche, l'entrepreneur devra produire une boîte à outils pour l'auto-évaluation de la cybersécurité, comprenant des outils d'évaluation (tâches 5.3.3 et 5.3.3) et des guides d'utilisation pour ces outils (5.3.5). Une orientation supplémentaire visant à aider les administrations routières à comprendre comment et quand utiliser les outils dans le cadre d'un programme de gestion des risques et d'amélioration de la cybersécurité est présentée à la tâche 5.4.

L'entrepreneur devra faire la démonstration de la boîte à outils et la mettre à jour après les séances de consultation des parties prenantes, conformément à la tâche 5.5.1.

5.3.1 Document de conception et questionnaire (outil d'évaluation du profil actuel et du profil cible de la cybersécurité)

Conformément au plan élaboré dans le cadre de la tâche 5.2.2, l'entrepreneur doit rédiger et soumettre des documents de conception détaillés qui décrivent le format, les questions, les commentaires, les résultats, la structure, le processus, la logique et d'autres renseignements pertinents, avant de concevoir les outils.

Les documents de conception comprendraient toutes les questions à intégrer dans les outils, ainsi que le modèle de logique ou de processus montrant la relation entre les questions, les commentaires des utilisateurs et les résultats générés.

5.3.2 Créer un outil pour l'évaluation du profil actuel de la cybersécurité adapté aux opérations des SGT et aux infrastructures connexes. Un guide d'utilisateur doit également accompagner l'outil (consulter 5.3.5).

L'objectif de l'outil est d'aider les administrations routières à déterminer leur état actuel en matière de cybersécurité et de gestion des risques. Ces renseignements serviront de base de référence à partir de laquelle l'organisation pourra déterminer où intervenir. L'outil doit :

- a) aiguiller l'utilisateur dans l'établissement des priorités et le choix de la portée des opérations, des systèmes, des actifs et des exigences réglementaires aux fins de l'évaluation;
- b) guider l'utilisateur, au moyen d'un **questionnaire** détaillé et complet, à déterminer l'état de préparation actuel de l'organisation en matière de cybersécurité, en tenant compte, au minimum, des données suivantes :
 - I. les objectifs et les priorités opérationnels et ceux de la mission;
 - II. les types d'équipements et de services des systèmes de transport intelligents déployés, notamment la connexion réseau entre les appareils et les SGT, ainsi que la topologie, la segmentation et les sauvegardes du réseau, avec une attention particulière aux technologies augmentant le niveau de connectivité ou d'automatisation des SGT;
 - III. le contexte des menaces;
 - IV. la taille et la complexité opérationnelles;
 - V. les exigences réglementaires ou juridiques;
 - VI. les pratiques d'échange de renseignements;
 - VII. les exigences de cybersécurité de la chaîne d'approvisionnement;
 - VIII. les contraintes organisationnelles;

IX. chaque catégorie et sous-catégorie de l'annexe A du cadre de sécurité du NIST.

- c) L'outil doit fournir des options par défaut à sélectionner (qui sont suggérées) et des options personnalisables concernant les commentaires des points 5.3.1 b).
- d) L'outil d'évaluation doit orienter l'utilisateur dans l'application des principes du cadre de sécurité du NIST et des autres ressources énumérées à l'annexe B à leur contexte opérationnel. Par exemple, l'outil d'évaluation peut reposer sur les questions utilisées dans le *Cyber Resilience Review Self-Assessment Package* (en anglais seulement), mais les questions doivent être peaufinées pour aider l'utilisateur à comprendre comment il doit les appliquer aux SGT, avec des exemples illustrés, le cas échéant.
- e) L'outil d'évaluation doit générer un résultat ou un document concernant le profil actuel ainsi qu'un rapport de synthèse comprenant les éléments suivants :
- I. un aperçu du niveau de maturité de la mise en œuvre pour chaque sous-catégorie du cadre de sécurité du NIST (p. ex. non mis en œuvre, partiellement mis en œuvre, majoritairement mis en œuvre, ou entièrement mis en œuvre);
 - II. une évaluation quantitative (p. ex. une note sur 10) du rendement global de l'organisation dans chaque fonction du cadre de sécurité du NIST;
 - III. une évaluation du niveau global de l'organisation en ce qui concerne la mise en œuvre du cadre de sécurité du NIST;
 - IV. des rétroactions qualitatives concernant l'état de préparation, les capacités, les aptitudes, les lacunes et les efforts d'amélioration recommandés de l'organisation.

5.3.3 Créer un outil d'évaluation du profil cible de la cybersécurité adapté aux opérations des SGT et aux infrastructures connexes. Un guide d'utilisateur doit également accompagner l'outil (consulter 5.3.5).

L'objectif de l'outil est d'aider l'organisation à déterminer l'état *souhaité* (cible) en matière de cybersécurité et de gestion des risques. L'outil doit comprendre ce qui suit :

- a) un questionnaire supplémentaire qui aidera l'organisation à déterminer son profil cible de cybersécurité et l'état de sa gestion des risques, en tenant compte, au minimum, des données suivantes :
- I. les résultats souhaités en matière de cybersécurité;
 - II. la tolérance aux risques;
 - III. les ressources;
 - IV. le contexte des menaces;
 - V. la stratégie de gestion des risques;
 - VI. les résultats de l'évaluation des risques du profil actuel;
 - VII. le profil actuel et le niveau de mise en œuvre du cadre de sécurité du NIST;
 - VIII. les exigences réglementaires ou juridiques;
 - IX. les pratiques d'échange de renseignements;
 - X. les objectifs et les priorités opérationnels et ceux de la mission;
 - XI. les exigences de cybersécurité de la chaîne d'approvisionnement;
 - XII. les contraintes organisationnelles.

-
- b) L'outil doit fournir des options par défaut à sélectionner (qui sont suggérées) et des options personnalisables concernant les commentaires des points 5.3.3 b).
- c) L'outil doit permettre l'importation d'un profil cible par défaut comme référence (qui comprend des considérations pour les opérations pilotes de VCA).
- d) L'évaluation doit orienter l'utilisateur dans l'application des principes du cadre de sécurité du NIST et des autres ressources énumérées au point 5.1.1 à leur contexte opérationnel dans le domaine des transports et aux résultats escomptés liés à l'établissement d'un profil cible approprié en matière de cybersécurité.
- e) L'outil d'évaluation doit générer un résultat ou un document concernant le profil cible ainsi qu'un rapport de synthèse comprenant les éléments suivants :
- I. un aperçu des catégories et des sous-catégories du cadre de sécurité du NIST ainsi que le niveau à atteindre (p. ex. non mis en œuvre, partiellement mis en œuvre, majoritairement mis en œuvre, ou entièrement mis en œuvre);
 - II. une évaluation quantitative (p. ex. une note sur 10) du rendement cible global de l'organisation dans chaque fonction du cadre de sécurité du NIST;
 - III. une évaluation du niveau global de l'organisation en ce qui concerne la mise en œuvre cible du cadre de sécurité du NIST;
 - IV. des rétroactions qualitatives générées concernant l'état de préparation, les capacités, les aptitudes, les lacunes et les efforts d'amélioration recommandés de l'organisation.

5.3.4 Exigences de conception communes pour les points 5.3.2 et 5.3.3

- a) L'outil doit fonctionner comme un produit autonome sur un seul ordinateur (c'est-à-dire l'ordinateur de l'utilisateur) et ne doit pas avoir besoin de maintenance ou de soutien supplémentaire de la part du développeur au fil des ans. L'outil doit être convivial et observer les pratiques exemplaires de l'expérience utilisateur (UX).
- b) Les outils d'évaluation du profil actuel et du profil cible en matière de cybersécurité peuvent être fournis en tant que solution combinée à condition que les exigences des points 5.3.32 et 5.3.3 soient respectées. Le type de logiciel ou de fichier (p. ex. Excel, Adobe Acrobat ou sur le Web [HTML]) sera déterminé avec le responsable technique. **La décision finale concernant le format relève de Transports Canada.**
- c) Les outils ne doivent pas faire la gestion et la maintenance du stockage des données de l'utilisateur (c'est-à-dire qu'ils ne stockent pas les données de l'utilisateur dans une base de données).
- d) Grâce aux outils, les utilisateurs doivent pouvoir sauvegarder ou exporter hors connexion leurs évaluations finales et celles en cours et doivent pouvoir les charger ou les importer ultérieurement, conformément aux normes de sécurité appropriées et aux pratiques exemplaires de l'industrie, comme il a été déterminé avec le responsable technique du projet.
- e) La portion questionnaire des outils doit être adaptée aux opérations des SGT et à l'infrastructure associée. Elle doit aussi être adaptée selon un niveau de détail technique et présenter un langage clair auquel un ingénieur ou un technicien type de la circulation serait en mesure de répondre sans connaissances particulières sur la cybersécurité et les systèmes informatiques.

-
- f) Les outils doivent pouvoir être personnalisés, notamment par l'ajout de nouvelles questions, la modification des questions existantes et la flexibilité dans le choix de la portée de l'évaluation.

5.3.5 Guides d'utilisateur (outil d'évaluation du profil actuel et du profil cible de la cybersécurité)

- a) Rédiger et soumettre des guides d'utilisateur qui fournissent des instructions détaillées sur l'utilisation des outils (tâches 5.3.32 et 5.3.3), et fournir des explications ou des considérations supplémentaires en répondant à chaque question, notamment en fournissant des exemples illustrés, le cas échéant, sur l'application de cette question au contexte des SGT. Une telle orientation aidera l'utilisateur à se servir des outils, tandis que celle de la tâche 5.4 l'aidera à utiliser les renseignements générés par les outils pour développer ou améliorer un programme de cybersécurité conforme au point 3.2 du cadre de sécurité du NIST.
- b) L'orientation doit comprendre des renseignements et les pratiques exemplaires sur la manière de planifier, de structurer et de réaliser les évaluations; citons notamment la création d'une équipe interfonctionnelle qui représentera convenablement les groupes organisationnels nécessaires, tels que les entreprises, les opérations, la sécurité, les TI et la maintenance.
- c) L'orientation doit comprendre les renseignements et les pratiques exemplaires sur la définition de la portée des évaluations dans les zones de sécurité appropriées, conformément à l'approche du niveau d'assurance de la sécurité du NIST et au modèle de Purdue pour les systèmes de contrôle industriels (SCI).
- d) L'orientation doit aider l'utilisateur à comprendre et à déterminer son contexte de menaces (5.3.2 b III, 5.3.3 a IV).

5.4 Orientation pour l'élaboration et la mise en œuvre d'un programme d'amélioration de la cybersécurité pour les opérations des SGT et les infrastructures connexes

5.4.1 Élaborer une orientation visant à fournir aux administrations routières des instructions détaillées sur la manière de créer et de mettre en œuvre un programme et un plan d'action en matière de cybersécurité (cadre de sécurité du NIST 3.2, étapes 1 à 7).

Cette orientation reposerait sur les ressources existantes, à savoir le point 3.2 du cadre de sécurité du NIST et ISO 27001 – *Systèmes de management de la sécurité de l'information*, et sur d'autres pratiques exemplaires pertinentes du secteur. Elle serait adaptée aux opérations des SGT, aux infrastructures et aux administrations routières de façon plus générale. Dans le *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance*² (en anglais) figure un exemple du type privilégié d'orientation et de personnalisation propre au secteur dans le cadre de cette tâche. L'orientation doit être aussi détaillée que le code de pratique ISO 27002 pour ce qui est des contrôles de sécurité de l'information, mais doit présenter un langage technique clair qu'un ingénieur ou un technicien type de la circulation pourra comprendre.

Le format choisi pour l'orientation (p. ex. un rapport ou une série de courts documents) sera déterminé avec le responsable technique.

L'orientation doit comprendre :

- a) les instructions de mise en œuvre pour chaque étape du point 3.2 portant sur l'établissement ou l'amélioration d'un programme de cybersécurité, dans la version 1.1 du cadre de sécurité du NIST (ou la section équivalente d'une version plus récente s'il y a lieu).

Remarque : L'orientation ferait référence à l'outil créé dans la tâche 5.3.2 de l'étape 3, et à celui de la tâche 5.3.35.3.35.3.3 de l'étape 5.

- b) Information et pratiques exemplaires sur la manière de planifier, de structurer et de réaliser le programme de cybersécurité, notamment la création d'une équipe interfonctionnelle qui représentera convenablement les groupes organisationnels nécessaires, tels que les entreprises, les opérations, la sécurité, les TI et la maintenance.
- c) Informations et pratiques exemplaires sur la définition de la portée et l'orientation du programme (Cadre de sécurité du NIST 3.2, étapes 1 et 2) pour assurer la cohérence avec les évaluations et conformément à l'approche du niveau d'assurance de la sécurité du NIST et au modèle de Purdue pour les systèmes de contrôle industriels (SCI).
- d) Orientations et pratiques exemplaires sur les éléments suivants, adaptées aux activités et à l'infrastructure du système de gestion de la circulation (SGC) :
- I. Gestion des actifs et tenue de documents sur l'architecture;
 - II. Gouvernance, leadership et attribution des responsabilités;
 - III. Création de l'environnement d'affaires et d'une politique de sécurité de l'information;
 - IV. Évaluations des risques et de la vulnérabilité;
 - V. Stratégie de gestion des risques;
 - VI. Gestion de la chaîne d'approvisionnement;
 - VII. Acquisition, développement et intégration de systèmes;
 - VIII. Gestion de l'identification, authentification et contrôle d'accès;
 - IX. Ressources humaines, formation et sensibilisation pour les différents rôles opérationnels du SGC;
 - X. Sécurité des données;
 - XI. Processus et procédures de protection des renseignements;
 - XII. Sécurité matérielle;
 - XIII. Sécurité des opérations;
 - XIV. Sécurité des communications;
 - XV. Entretien;
 - XVI. Technologie protectrice;
 - XVII. Détection des anomalies et des événements;
 - XVIII. Surveillance en continu de la sécurité;
 - XIX. Maintenance et mise à l'essai des processus de détection;
 - XX. Planification des interventions;
 - XXI. Communication et coordination des activités d'intervention;
 - XXII. Gestion des incidents;
 - XXIII. Gestion de la continuité des activités;
 - XXIV. Analyse de l'intervention aux incidents et de la reprise;
 - XXV. Atténuation des événements et de leurs effets;
 - XXVI. Planification de la reprise;

- XXVII. Communication et coordination des activités de reprise;
 XXVIII. Vérification interne et amélioration continue.

- e) Information sur la manière d'appliquer et d'analyser les résultats (profil actuel et profil cible) des outils (Tâche 5.3) pour comparer les profils actuel et cible du Cadre de sécurité du NIST 3.2 (étapes 3 et 5).
- f) Information sur la tenue d'une évaluation des risques fondée sur les résultats de l'outil sur le profil actuel conformément au Cadre de sécurité du NIST 3.2 (étape 4).
- g) Information sur l'élaboration d'un plan d'action des priorités selon le Cadre de sécurité du NIST 3.2 (étape 6) pour combler les écarts entre le profil actuel et le profil cible. Ce plan d'action est basé sur les résultats de l'analyse des résultats des outils du profil actuel et du profil cible décrits au point 5.4.1 (e) et les résultats de l'évaluation des risques au point 5.4.1 (f).
- h) Recommandations et des orientations propres à la technologie V2X et au SGC, notamment : les circonstances où les renvois à titre indicatif au NIST (normes, lignes directrices et pratiques) doivent être pris en compte, leur application à l'élaboration d'un programme d'amélioration de la cybersécurité (Cadre de sécurité du NIST 3.2 étapes 1 à 7), et l'application d'une approche d'ingénierie des systèmes en vue de l'architecture, de la conception, du déploiement et de la maintenance de l'infrastructure et des produits de SGC (normes NIST 800-160 et ISO 15288).
- i) Information sur l'adaptation et le ciblage du programme d'amélioration de la cybersécurité pour mettre en œuvre le plan d'action (Cadre de sécurité du NIST 3.2, étape 7) du point 5.3.3 (g) et la répétition interactive des étapes 1 à 7 aux fins de l'amélioration continue.
- j) Tenue d'une étude de cas d'un SGC typique, montrant des exemples concrets pour les étapes 1 à 7 du Cadre de sécurité du NIST 3.2, y compris la manière d'appliquer les outils et les résultats à un cas d'utilisation réel.

5.5 Consultation des intervenants, soutien technique, formation et révision de la boîte à outils d'évaluation de la cybersécurité et des documents d'orientation du programme d'amélioration de la cybersécurité

Des séances de consultation des intervenants et de soutien technique sur place seront organisées, et permettront de recueillir les commentaires des utilisateurs sur la boîte à outils (tâche 5.3) et des conseils de cybersécurité (tâche 5.4). L'entrepreneur révisera la boîte à outils d'évaluation de la cybersécurité et les documents d'orientation sur la cybersécurité à la lumière des enseignements tirés de ces séances.

5.5.1 Consultation des intervenants

Organiser et diriger des séances de consultation avec les intervenants (qui seront précisés par Transports Canada) afin de présenter la boîte à outils d'évaluation de la cybersécurité (tâche 5.3) et les documents d'orientation sur la cybersécurité (tâche 5.4) et de recueillir des commentaires à leur sujet, et rassembler les pratiques exemplaires existantes en matière de cybersécurité appliquées par les intervenants.

5.5.1.1 Tenir un maximum de trois (3) séances de consultation de groupe (des séances de consultation supplémentaires pourraient être ajoutées conformément à l'option 1 du contrat – tâche 5.6.1). Deux (2) de ces séances peuvent être faites par webinaire. Sous réserve d'un assouplissement des restrictions de voyage causées par la pandémie de COVID-19, une des séances de consultation sera menée en personne à un endroit au Canada choisi par Transports Canada. Si cela n'est pas possible, cette séance sera également menée de manière virtuelle. Les frais de déplacements et de prestation de services de consultation seront remboursés conformément aux points 12 et 18.4, respectivement.

5.5.1.2 Mener un maximum de quinze (15) séances de consultation ciblées (c'est-à-dire des entretiens avec des organisations particulières plutôt que des séances de groupe).

5.5.1.3 Élaborer du matériel pour les séances, y compris l'ordre du jour et les diapositives de présentation.

5.5.2 Soutien technique sur place

Organiser, diriger et fournir le soutien technique à trois (3) administrations routières dans la tenue d'une évaluation de la cybersécurité au moyen de la boîte à outils développée à la tâche 5.3 et mettre en œuvre un programme d'amélioration de la cybersécurité en utilisant les documents d'orientation créés à la tâche 5.4.

Le soutien technique peut inclure l'offre d'orientations et de formations supplémentaires sur l'utilisation des outils et l'aide à l'analyse propre à la configuration et aux activités du SGC évalué. Pour chacun des trois (3) emplacements de l'administration routière, l'entrepreneur fournira un minimum de quatre (4) jours de soutien technique en personne (à un endroit au Canada qui sera choisi par Transports Canada) et cinq (5) jours de soutien technique à distance supplémentaires. Les frais de déplacement seront remboursés conformément au point 12.

5.5.3 Apporter des révisions à la boîte à outils d'évaluation de la cybersécurité (tâche 5.3) et aux documents d'orientation sur la cybersécurité (tâche 5.4).

5.5.3.1 Rédiger un résumé de la rétroaction obtenue lors des séances de consultation, des enseignements tirés de la mise en œuvre et du soutien ainsi que des changements proposés à la boîte à outils et aux documents d'orientation.

5.5.3.2 Achever les révisions de la boîte à outils et des documents d'orientation, comme convenu avec le responsable technique.

5.5.4 Formation

5.5.4.1 Élaborer une formation de trois jours et les documents de présentation connexes à l'intention du personnel des administrations routières (par exemple, les ingénieurs de la circulation ou des STI, les planificateurs des transports, les techniciens en TI) pour donner un aperçu de la manière d'utiliser la boîte à outils d'évaluation de la cybersécurité (tâche 5.3) et les documents d'orientation sur la cybersécurité (tâche 5.4). Les frais de déplacement seront remboursés conformément au point 12.

5.5.4.2 Créer une version virtuelle de la formation qui pourrait être offerte exclusivement en ligne en trois à six séances d'une demi-journée.

5.5.4.3 Organiser (y compris en obtenant des installations et de l'équipement audiovisuel, en assurant l'accueil des participants et en réglant d'autres aspects logistiques), animer et fournir six (6) séances de formation en personne ou virtuellement.

Sous réserve d'un assouplissement des restrictions de voyage causées par la pandémie de COVID-19, ces séances seront menées en personne à des endroits au Canada et à des moments choisis par Transports Canada. Les frais de déplacement seront remboursés conformément au point 12.

Chaque séance de formation sur place doit pouvoir accueillir 30 participants en personne et 100 participants à distance supplémentaires par webinaire. Chaque séance de formation virtuelle doit permettre d'accueillir 150 participants à distance.

Les frais de présentation de la séance de formation seront remboursés conformément au point 18.

5.6 Tâches optionnelles – en fonction d'autorisations de tâches requises en fonction des besoins

Lorsque le responsable technique demande un projet dans le cadre des options du contrat, l'entrepreneur doit être disponible dans les deux semaines suivant la demande du responsable technique pour discuter des tâches et des livrables précis.

À la demande du responsable technique, l'entrepreneur doit soumettre un document relatif à la portée des travaux dans un délai de deux semaines, lequel comprendra :

- a) un plan de travail du projet;
- b) les grandes lignes du projet;
- c) le calendrier des conférences téléphoniques;
- d) le calendrier des délais pour les présentations provisoires et définitives;
- e) le contenu et les activités du projet;
- f) le budget.

La portée des travaux de chaque projet doit être approuvée par l'autorité contractante par écrit avant le début de tout travail en vertu de ces options par une autorisation de tâches approuvée (annexe H).

5.6.1 Tâche optionnelle 1 : Consultation supplémentaire, soutien technique et formation au besoin

Le travail demandé aux termes de cette option sera fait au fur et à mesure des besoins, en fonction d'un formulaire d'autorisation de tâches. Cela peut inclure des consultations, du soutien technique ou une formation supplémentaires, conformément à la tâche 5.5, afin d'appuyer davantage l'utilisation de la boîte à outils d'évaluation de la cybersécurité (tâche 5.3) et du document d'orientation du programme d'amélioration de la cybersécurité (tâche 5.4) par les intervenants canadiens.

5.6.2 Tâche optionnelle 2 : Analyse de la vulnérabilité de la cybersécurité (à l'exclusion des tests de pénétration) et conseils stratégiques au fur et à mesure des besoins.

Le travail demandé aux termes de cette option sera fait au fur et à mesure des besoins, en fonction d'un formulaire d'autorisation de tâches. Cela peut comprendre des simulations, l'examen des spécifications techniques et pour l'équipement, de la documentation sur les technologies émergentes, des architectures systèmes et réseaux et la fourniture d'analyses, de conseils stratégiques ou de rapports à Transports Canada ou à ses intervenants (par exemple, les administrations routières) sur des questions particulières.

Les livrables peuvent prendre la forme de rapports, de séances d'information, de fiche de renseignements, de présentations, d'enquêtes, de participation à des réunions et d'ateliers ou de tables rondes à l'appui.

5.6.3 Tâche optionnelle 3 : Tests de pénétration, analyse des vulnérabilités et identification des exploits des systèmes et de l'équipement, fournis au fur et à mesure des besoins.

On s'attend à ce que l'entrepreneur ait accès aux installations, à l'expertise et à l'équipement nécessaires pour effectuer les travaux décrits dans cette option.

Le travail demandé aux termes de cette option sera fait au fur et à mesure des besoins, en fonction d'un formulaire d'autorisation de tâches. Cela peut comprendre des tests de pénétration, des analyses de vulnérabilité, l'identification des exploits et la présentation de recommandations sur les mesures d'atténuation pour divers réseaux et équipements de véhicules et de SGC (par exemple, contrôleur de feux de circulation, caméras et infrastructure connexe, GPS et dispositifs de chronométrage, panneaux de limitation de vitesse variable, etc.) afin d'étayer les orientations sur l'atténuation des risques de cybersécurité.

D'autres tâches demandées dans cette option peuvent également comprendre :

- a) Recueillir et examiner l'information afin de caractériser l'équipement et de préparer les tests de vulnérabilité;
- b) Configurer les sous-systèmes des véhicules et du SGC en laboratoire pour préparer les tests;
- c) Réaliser des essais sur le terrain sur demande ou au besoin;
- d) Mettre à l'essai les mesures d'atténuation recommandées;
- e) Évaluer l'applicabilité et les lacunes des normes et des protocoles de cybersécurité;
- f) Élaborer des procédures pour les essais de cybersécurité.

Aux fins de la préparation de la soumission, le soumissionnaire peut supposer que les achats de matériel à tester auront lieu en consultation avec Transports Canada et seront remboursés conformément au point 20.

6 Produits livrables et calendrier du projet

Tableau 1 : Produits livrables du projet et estimation du calendrier en semaines à compter de la date d'attribution du contrat

Point	Tâche	Produits livrables	Échéancier (au cours des X semaines suivant l'attribution du contrat)
Plan de projet, analyse documentaire, abécédaire de la cybersécurité dans les transports routiers, documents d'information, plan de la boîte à outils d'évaluation de la cybersécurité			
1	5.1	Tâche 5.1 – Plan de gestion du projet	2 (et mises à jour continues)
2	5.2	Livrables des tâches 5.2.1 à 5.2.5 – versions provisoires : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ.	6
		<i>Vérification par TC et rétroaction</i>	9
3	5.2	Livrables des tâches 5.2.2 à 5.2.5 – versions révisées : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ.	12
		Rapport sur la résolution des commentaires. <i>Vérification par TC et rétroaction</i>	15
4	5.2	Livrables des tâches 5.2.2 à 5.2.5 – versions définitives : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ.	18
		Rapport sur la résolution des commentaires. <i>Vérification par TC et rétroaction</i>	19
5	5.2	Livrables des tâches 5.2.6 et 5.2.7 – Six séances de formation virtuelle et webinaire enregistré.	À déterminer
Outils d'évaluation de la cybersécurité			
6	5.3	Livrables de la tâche 5.3.1 – versions provisoires : document de conception et questionnaire.	23
		<i>Vérification par TC et rétroaction</i>	26
7	5.3	Livrables de la tâche 5.3.1 – versions révisées : document de conception et questionnaire.	28
		<i>Vérification par TC et rétroaction</i>	31
8	5.3	Livrables de la tâche 5.3.1 – versions définitives : document de conception et questionnaire.	33
		<i>Vérification par TC et rétroaction</i>	34
9	5.3	Prototype de boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3), version provisoire du guide de l'utilisateur (tâche 5.3.5), et démonstration de la boîte à outils par webinaire.	40
		<i>Vérification par TC et rétroaction</i>	44

Point	Tâche	Produits livrables	Échéancier (au cours des X semaines suivant l'attribution du contrat)
10	5.3	Version révisée de la boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3) et du guide de l'utilisateur (tâche 5.3.5), et démonstration de la boîte à outils par webinaire et résumé de la résolution des commentaires.	48
		<i>Vérification par TC et rétroaction</i>	52
11	5.3	Version définitive de la boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3) et du guide de l'utilisateur (tâche 5.3.5), et démonstration de la boîte à outils par webinaire et résumé de la résolution des commentaires.	54
		<i>Vérification par TC et rétroaction</i>	56
Orientation sur l'auto-évaluation de la cybersécurité			
12	5.4	Livrable de la tâche 5.4.1 – aperçu de l'orientation.	57
		<i>Vérification par TC et rétroaction</i>	59
13	5.4	Livrable de la tâche 5.4.1 – version provisoire de l'orientation.	69
		<i>Vérification par TC et rétroaction</i>	72
14	5.4	Livrable de la tâche 5.4.1 – version révisée de l'orientation et rapport sur la résolution des commentaires.	77
		<i>Vérification par TC et rétroaction</i>	80
15	5.4	Livrable de la tâche 5.4.1 – version définitive* de l'orientation et rapport sur la résolution des commentaires. * consultation préalable	83
		<i>Vérification par TC et rétroaction</i>	84
Consultation des intervenants, soutien technique sur place, formation			
16	5.5	Tâche 5.5.1.1 – versions provisoires des ordres du jour et des diapositives de présentation pour les séances de consultation.	85
		<i>Vérification par TC et rétroaction</i>	86
17	5.5	Tâche 5.5.1.1 – versions définitives des ordres du jour et des diapositives de présentation pour les séances de consultation.	86
		<i>Vérification par TC et rétroaction</i>	87
18	5.5	Tâche 5.5.1 – Fourniture de trois séances sessions de consultation de groupe des intervenants et de 15 séances individuelles sur la boîte à outils (tâche 5.3) et l'orientation (tâche 5.4).	89
19	5.5	Tâche 5.5.2 – Offre de services de soutien technique sur place et à distance à trois administrations routières.	92
20	5.5	Tâche 5.5.3.1 – Résumé de la rétroaction obtenue lors des séances de consultation, des enseignements tirés de la mise en œuvre et du soutien ainsi que des changements proposés à la boîte à outils et aux documents d'orientation.	93
		<i>Vérification par TC et rétroaction</i>	94
21	5.5	Tâche 5.5.3.2 – versions révisées de la boîte à outils et des documents d'orientation.	97
		<i>Vérification par TC et rétroaction</i>	100
22	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions provisoires des ordres du jour, du matériel de formation et des diapositives de présentation.	103

Point	Tâche	Produits livrables	Échéancier (au cours des X semaines suivant l'attribution du contrat)
		<i>Vérification par TC et rétroaction</i>	106
23	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions révisées des ordres du jour, du matériel de formation et des diapositives de présentation, et rapport de résolution des commentaires.	108
		<i>Vérification par TC et rétroaction</i>	109
24	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions définitives des ordres du jour, du matériel de formation et des diapositives de présentation, et rapport de résolution des commentaires.	111
25	5.5	Tâche 5.5.4.3 – Tenue de six séances de formation.	À déterminer

7 Langue de travail

La principale langue de communication, à l'oral et à l'écrit, sera l'anglais. Transports Canada facilitera la traduction si nécessaire et en assumera les coûts.

8 Lieu de travail

Le travail doit être effectué dans les locaux de l'entrepreneur. Des déplacements au Canada et aux États-Unis pourraient être nécessaires pour organiser des réunions, mener des séances de consultation, fournir de la formation, mener des essais et offrir un soutien technique. Le lieu des réunions, des séances de consultation et de formation et du soutien technique sur place sera déterminé par le responsable technique.

Les travaux qui nécessitent l'accès à de l'information de niveau Protégé B ou leur traitement peuvent être effectués sur le lieu d'activité de l'entrepreneur après que les zones de travail requises ont été approuvées.

Au besoin, le travail effectué dans le cadre des tâches 5.6.2 et 5.6.3 qui nécessite l'accès ou le traitement de renseignements de niveau secret sera effectué dans des installations appropriées du gouvernement du Canada, et les frais de déplacement seront remboursés conformément au point 14.

9 Format des produits livrables

À moins d'indication contraire aux points 5 ou 6, tous les produits livrables doivent être fournis en version électronique compatible avec MS Word ou MS PowerPoint, en anglais.

Les présentations, les aperçus, les rapports provisoires et définitifs doivent être soumis en anglais seulement.

10 Durée du contrat

La « **durée du contrat** » désigne la période entière pendant laquelle l'entrepreneur doit exécuter les travaux, et comprend :

- I. La « **période initiale du contrat** », qui commence à la date d'attribution du contrat jusqu'au le 31 mars 2024 (a fin des tâches 5.1-5.5 telles qu'identifiées dans les sections 5 et 6; et la période pendant laquelle le contrat est prolongé, si le Canada choisit d'exercer;

- II. Toutes les options énoncés dans la tâche optionnelle 1 (tâche 5.6.1), la tâche optionnelle 2 (5.6.2) et la tâche optionnelle 3 (tâche 5.6.3), telles qu'identifiées dans les sections 5 et 6.

Prorogation du contrat :

Le Canada peut se prévaloir des tâches optionnelles n'importe quand avant la fin de la durée du contrat, par une note écrite à l'entrepreneur. Le Canada peut exercer simultanément toute combinaison de tâches optionnelles. Les tâches optionnelles peuvent être exercées uniquement par l'autorité contractante, et seront attestées, à des fins administratives, au moyen d'une autorisation de tâches officielle.

11 Niveau d'effort

Le niveau d'effort *estimé* pour les tâches 5.1 à 5.5 est de 560 jours-personnes pendant la période allant de l'attribution du contrat à mars 2024.

12 Déplacements

Des déplacements seront nécessaires pour assister à des réunions, mener des séances de consultation, fournir de la formation, mener des essais et offrir un soutien technique, comme l'indiquent les points 5 et 6. Les frais de déplacement doivent être inclus dans le prix du contrat et seront payés conformément aux dispositions applicables énoncées dans la base de paiement.

L'entrepreneur sera remboursé pour les frais autorisés de déplacement réels raisonnablement engagés dans l'exécution des travaux, au prix coûtant, sans aucune indemnité pour les frais généraux ou les bénéfiques, conformément aux indemnités relatives aux repas, à l'hébergement et à l'utilisation d'un véhicule privé qui sont précisées aux appendices B, C et D de la *Directive sur les voyages* du Conseil national mixte et selon les autres dispositions de la *Directive* qui se rapportent aux « voyageurs » plutôt que celles qui se rapportent aux « employés ». Le Canada ne versera à l'entrepreneur aucune indemnité de faux frais pour les voyages autorisés.

Tout voyage doit être autorisé au préalable par Transports Canada au moyen d'une autorisation de voyage.

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Remarque sur la préparation des soumissions :

- a) **Le soumissionnaire doit joindre une estimation des frais de déplacement de 25 000 \$ pour les dépenses remboursables sur présentation d'un reçu.**
- b) **Le coût du temps de déplacement du personnel de l'entrepreneur doit être pris en compte dans le prix concurrentiel des tâches 5.1 à 5.5, en supposant deux jours de temps de déplacement (un jour dans chaque direction) pour chaque déplacement et chaque ressource requise. Le temps de déplacement supplémentaire du personnel pour les travaux relevant des options de la tâche 5.6 sera pris en compte dans le budget défini en fonction des besoins.**

13 Propriété intellectuelle

Transports Canada a déterminé que tout droit de propriété intellectuelle découlant de l'exécution des travaux prévus par le contrat sera dévolu au Canada, pour les motifs suivants :

-
- Le marché d'acquisition de l'État ou les produits livrables aux termes du contrat visent principalement à produire des connaissances et des renseignements qui seront diffusés au public.

14 Exigences en matière de confidentialité

L'expression « renseignements confidentiels » s'entend de tout renseignement (verbal, écrit ou informatique), qualifié, oralement ou par écrit, de renseignement de nature « confidentielle », « restreinte » ou « protégée », ce qui englobe les extraits et les copies de ces renseignements et les notes prises par l'expert-conseil dans le cadre de l'examen de ces documents.

L'expert-conseil doit :

- S'abstenir de reproduire, sous quelque forme que ce soit, l'une ou l'autre des parties de la documentation ou de la démonstration considérées comme exclusives par Transports Canada ou d'autres participants au projet;
- Traiter de la façon la plus confidentielle tout renseignement confidentiel obtenu et ne pas divulguer ces renseignements à quiconque, excepté aux membres directs de l'équipe du projet, au besoin;
- Prendre toutes les précautions nécessaires dans le traitement de l'information, de manière à éviter que toute personne non autorisée y ait accès.

15 Renseignements de nature délicate sur le plan commercial

L'information fournie dans le cadre du processus pourrait comprendre de l'information de nature délicate sur le plan commercial.

Tout renseignement fourni dans ce processus sera protégé contre la divulgation dans la mesure permise par la loi. L'entrepreneur veillera à ce que la façon dont il traite les données confidentielles, exclusives et de nature délicate sur le plan du marché fournies par Transports Canada et d'autres sources protège les intérêts des sources.

Avant de recevoir les données ou l'information, l'entrepreneur doit conclure une entente officielle avec Transports Canada sur le traitement, l'utilisation et l'élimination définitive des données.

16 Exigences d'attestation de sécurité

Les ressources travaillant sur les tâches 5.1 à 5.5 et sur la tâche 5.6.1 peuvent avoir besoin d'accéder à des informations et des biens protégés et **DOIVENT donc être aptes à obtenir une COTE DE FIABILITÉ du gouvernement du Canada.**

Les ressources travaillant sur les tâches 5.6.2 et 5.6.3 peuvent avoir besoin d'accéder à des informations et des biens protégés ou classifiés et **DOIVENT donc être aptes à obtenir une cote de sécurité de niveau SECRET du gouvernement du Canada et avoir accès à un LIEU DE TRAVAIL qui est en mesure d'obtenir une cote PROTÉGÉ B du gouvernement du Canada.**

17 Acceptation

Tous les services et les travaux doivent satisfaire pleinement le responsable technique avant le paiement de la facture.

18 Gestion du projet

18.1 Gestion de projet

Le gestionnaire de projet de l'entrepreneur est chargé de ce qui suit :

- exercer l'autorité de signature du projet, superviser et assurer la qualité du travail et des produits livrables;
- gérer l'équipe de projet pendant les phases de planification, de mise en œuvre et de production de rapports des travaux;
- veiller à ce que le projet soit mis en œuvre conformément aux paramètres de délais, de coûts et de rendement convenus du contrat;
- rendre compte des progrès au responsable technique sur demande et aux étapes clés du cycle de vie décrit dans l'énoncé des travaux.

18.2 Administration du projet

Le responsable technique fournira à l'entrepreneur de la rétroaction au sujet des rapports d'étape et d'autres versions provisoires des livrables, et l'entrepreneur devra ensuite l'intégrer à ses livrables définitifs. Les commentaires sur les rapports définitifs ou autres livrables doivent être pris en compte, et ces rapports et livrables doivent être soumis à nouveau dans un délai d'une semaine suivant la réception des commentaires du responsable technique, par écrit. Le responsable technique s'emploiera à fournir ses commentaires dans les deux semaines suivant la réception des livrables provisoires, sous réserve des circonstances opérationnelles.

Tous les produits livrables devront être soumis dans le respect des échéances précisées au point 6. L'entrepreneur doit aviser dès que possible le responsable technique de tout retard prévu dans la présentation des produits livrables.

18.3 Soutien du projet

Transports Canada aidera à trouver les intervenants et les lieux appropriés pour les séances de consultation (tâche 5.5.1), le soutien technique et l'évaluation de la sécurité (tâche 5.5.2) et les séances de formation (tâche 5.5.4).

18.4 Organisation de séances de consultation et de formation des intervenants

L'entrepreneur sera remboursé pour les coûts autorisés liés au lieu, au service de réunion virtuel, à l'accueil et au matériel de consultation ou de formation raisonnables nécessaires pour assurer la tenue des séances, au prix coûtant, sans aucune indemnité supplémentaire pour les frais généraux ou la marge bénéficiaire.

Toutes les dépenses d'accueil et d'événements doivent être conformes à la Directive sur les dépenses de voyages, d'accueil, de conférences et d'événements du gouvernement du Canada et autorisées à l'avance par le responsable technique.

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Pour la préparation des soumissions, le soumissionnaire doit joindre une estimation des frais concernant le lieu, le service de réunion virtuel, l'accueil et le matériel de consultation, comme suit :

- **Tâche 5.5.1 : 10 000 \$.**
- **Tâche 5.5.4 : 15 000 \$ par séance de formation, pour un total de 90 000 \$.**

18.5 Matériel acheté pour les tests de pénétration (Tâche 5.6.3)

À l'achat d'équipement pour les tests prévus à cette tâche, l'entrepreneur sera remboursé au prix coûtant et raisonnable engagé pour l'achat de l'équipement autorisé, sans aucune indemnité supplémentaire pour les frais généraux ou la marge bénéficiaire. Tout achat d'équipement doit être autorisé par le responsable technique par écrit au préalable. **Aux fins de la préparation des soumissions, le soumissionnaire doit joindre une estimation des coûts de matériel de 50 000 \$.**

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Tous les appareils payés dans le cadre de cette tâche par le gouvernement du Canada demeurent la propriété du gouvernement du Canada. À la fin des tests ou à un moment précisé par le responsable technique, les dispositifs sont expédiés, aux frais du gouvernement, à un endroit déterminé par le responsable technique. L'entrepreneur doit utiliser l'emballage d'origine de l'appareil dans la mesure du possible et l'emballer de manière à éviter tout dommage pendant le transport.

19 Remplacement de ressources

L'entrepreneur doit fournir les services des personnes nommées dans le contrat, dotées des cotes de sécurité requises, pour l'exécution des travaux, à moins qu'il ne soit pas en mesure de le faire pour des raisons indépendantes de sa volonté.

Au cas où l'entrepreneur ne serait pas en mesure, à un moment quelconque, de fournir les services des ressources désignées dans le contrat, il devra alors fournir au même prix des remplaçants dans les cinq (5) jours suivant l'avis de remplacement; ces remplaçants doivent posséder des compétences et expériences égales ou supérieures et être acceptables aux yeux du responsable technique.

Avant la date prévue à laquelle le personnel de remplacement doit commencer les travaux, l'entrepreneur informera le responsable technique par écrit de la raison de la non-disponibilité des ressources nommées dans le contrat.

L'entrepreneur devra par la suite transmettre au responsable technique le ou les noms des personnes et un sommaire des qualifications et de l'expérience des remplaçants proposés, de même que leur cote de sécurité du gouvernement du Canada.

Les remplaçants seront évalués selon les critères d'évaluation initiale de la DP et en fonction des exigences relatives à la sécurité indiquées au point 16.

L'entrepreneur ne doit en aucun cas permettre à des remplaçants non autorisés par le responsable technique d'effectuer des services.

20 Imprévus

L'entrepreneur doit fournir un plan d'urgence au cas où, pendant l'affectation, l'une des ressources est indisponible à la suite de circonstances inévitables. Ce plan permettra de garantir que les délais des travaux requis par le responsable technique seront respectés.

Aucune obligation de payer pour des travaux non effectués en raison de la fermeture des bureaux du gouvernement :

- i. Si le fournisseur, ses employés, ses sous-traitants ou ses agents ne peuvent accéder aux locaux du gouvernement où ils assurent des services en vertu de la commande en raison de l'évacuation et de la fermeture de ces bureaux, et que cette situation les empêche de faire leur travail, le Canada

n'est pas tenu de payer le fournisseur pour les travaux qui auraient pu être effectués sans l'évacuation ou la fermeture;

ii. Si le fournisseur, ses employés, ses sous-traitants ou ses agents ne peuvent accéder aux locaux du gouvernement où ils assurent des services en vertu de la commande en raison d'une grève ou d'un lock-out, et que cette situation les empêche de faire leur travail, le Canada n'est pas tenu de payer le fournisseur pour les travaux qui auraient pu être effectués s'il avait eu accès aux locaux.

Annexe A – Glossaire

- a) **Administrations routières** : Ce terme désigne les organisations provinciales, territoriales et municipales qui sont responsables de la gestion des infrastructures routières, de la gestion de la circulation et des services de transport en commun.
- b) **Architecture** : Cadre de travail à l'intérieur duquel un système peut être bâti. Les besoins dictent les fonctionnalités auxquelles l'architecture doit répondre. Elle définit la fonctionnalité des composants d'un système et l'information échangée entre ces composants. Une architecture est orientée sur le plan fonctionnel, mais elle n'est pas particulière à une technologie, ce qui lui permet de rester efficace au fil du temps. Elle définit ce qui doit être fait, et non comment cela doit être fait.
- c) **Catégorie** : Sous-division d'une fonction en groupes de résultats en matière de cybersécurité, étroitement liés aux besoins des programmes et à des activités particulières. Parmi les exemples de catégories, citons la Gestion des actifs, la Gestion des identités et le contrôle des accès ainsi que les processus de détection (Cadre de sécurité du NIST, 2020).
- d) **Centre de gestion de la circulation** : Entité qui fournit des services d'application, de gestion, d'administration et de soutien à partir d'un lieu fixe qui n'est pas à proximité du réseau routier. Les termes « centre » et « service d'appui » sont utilisés de façon interchangeable. Le terme « centre » est traditionnellement axé sur le transport, évoquant les centres de gestion qui appuient les besoins en matière de transport, tandis que le terme « service d'appui » fait généralement référence aux applications commerciales (ARC-IT, 2020).
- e) **Communications centre à terrain** : Lien de communication entre des entités fixes, y compris des objets physiques centraux et des objets sur le terrain. Ce lien peut être mis en œuvre en utilisant divers réseaux et technologies de communication publics ou privés. Il peut s'agir, entre autres, de câbles à paires torsadées, de câbles coaxiaux, de fibres optiques, de réseaux de relais à micro-ondes, de réseaux cellulaires, de réseaux à spectre étalé, etc. L'essentiel de ce type de communications est de servir des objets fixes. Des ressources de communication dédiées et partagées peuvent être utilisées. Il s'agit de l'un des types d'interconnexion d'architecture définis dans l'ARC-IT (ARC-IT, 2020).
- f) **Communications entre le terrain et le véhicule (ou « infrastructure à véhicule » [I2V])** : Canal de communications sans fil utilisé pour les communications de proximité entre les véhicules et l'infrastructure immédiate. Il prend en charge les communications propres à un lieu pour les capacités des systèmes de transport intelligents telles que la perception des péages, la gestion des véhicules de transport en commun, l'information aux conducteurs et l'exploitation automatisée des véhicules commerciaux (ARC-IT, 2020).
- g) **Communications infrastructure à autre chose (I2X)** : Échange d'informations entre les infrastructures et d'autres éléments, y compris, notamment, la **communication entre les infrastructures et les véhicules, entre les infrastructures et les piétons et entre les infrastructures et d'autres infrastructures**.
- h) **Communications véhicule à autre chose (V2X)** : Échange d'information entre les véhicules et d'autres éléments, y compris, notamment, la **communication entre les véhicules et l'infrastructure, entre les véhicules et les piétons et entre les véhicules et d'autres véhicules** (Association des transports du Canada, 2020).
- i) **Communications véhicule à véhicule (V2V)** : Système sans fil dédié traitant un débit de données élevé, une faible probabilité d'erreur et des communications en visibilité directe entre les véhicules. Les services de véhicules avancés pourraient utiliser ce lien dans l'avenir pour appuyer la mise en œuvre de systèmes avancés de prévention des collisions, la communication

d'information sur l'état des routes et la coordination active avec les systèmes de contrôle avancés (ARC-IT, 2020).

- j) **Cybersécurité** : Processus de protection de l'information par la prévention, la détection et la réponse aux attaques (Cadre de sécurité du NIST, 2020).
- k) **Dispositif connecté V2X** : Tout appareil utilisé pour transmettre ou recevoir des messages d'un autre appareil. Un appareil connecté peut être catégorisé comme unité de bord, dispositif de sécurité après-vente ou unité en bord de route (ARC-IT, 2020).
- l) **Dispositif de sécurité après-vente** : Appareil connecté dans un véhicule qui fonctionne pendant que le véhicule est en mouvement, mais qui n'est pas connecté au bus de données du véhicule (Architecture Reference for Cooperative and Intelligent Transportation [ARC-IT], 2020).
- m) **Dispositifs sur le terrain** : Infrastructures intelligentes réparties à proximité du réseau de transport ou dans celui-ci qui remplissent des fonctions de surveillance (p. ex. détecteurs de circulation, caméras), de contrôle de la circulation (p. ex. contrôleurs de feux), d'information (p. ex. panneaux à messages variables) et de transaction locale (p. ex. péage, stationnement). En général, leur fonctionnement est régi par des fonctions de gestion des transports qui s'exercent en arrière-plan. Ils incluent également l'équipement en bordure de route et d'autres infrastructures de communication sans fil qui assurent les communications entre les éléments mobiles et les infrastructures fixes (ARC-IT, 2020).
- n) **Équipement de bord** : Modules informatiques, écran et unité de bord qui sont installés et intégrés dans les véhicules et fournissent une interface avec les capteurs du véhicule, ainsi qu'une interface de communication sans fil avec l'environnement routier et d'arrière-plan (ARC-IT, 2020).
- o) **Fonction** : La fonction est l'une des principales composantes du cadre. Les fonctions fournissent le niveau de structure supérieur pour l'organisation des activités de base en matière de cybersécurité en catégories et sous-catégories. Les cinq fonctions sont : Relever, Protéger, Détecter, Répondre et Récupérer (Cadre de sécurité du NIST, 2020).
- p) **Gestion des données** : Domaine concernant la gestion des données qui peuvent être utilisées par l'ensemble ou une partie des organismes de transport ou d'autres organisations pour appuyer la planification des transports, le suivi du rendement, l'analyse de la sécurité et la recherche. Les données sont collectées à partir de détecteurs et de capteurs, de véhicules connectés et de flux de données opérationnelles provenant des centres (ARC-IT, 2020).
- q) **Gestion des risques** : Processus d'identification, d'évaluation et de réponse aux risques (Cadre de sécurité du NIST, 2020).
- r) **Infrastructures essentielles** : Processus, systèmes, installations, technologies, réseaux, biens et services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et au bon fonctionnement du gouvernement. Il peut s'agir d'infrastructures indépendantes ou interconnectées et interdépendantes à l'intérieur des frontières du pays, d'une province ou d'un territoire ou entre ces endroits. Les perturbations des infrastructures essentielles peuvent entraîner des pertes de vie catastrophiques, avoir des effets néfastes sur l'économie et ébranler considérablement la confiance du grand public (principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada, Sécurité publique Canada, 2020).
- s) **Niveaux de mise en œuvre du cadre** : Optique par laquelle voir les caractéristiques de l'approche d'une organisation en matière de risque, c'est-à-dire la façon dont une organisation perçoit le risque en matière de cybersécurité et les processus mis en place pour gérer ce risque (Cadre de sécurité du NIST, 2020).

-
- t) **Noyau de cadre** : Ensemble d'activités et de références en matière de cybersécurité qui sont communes à tous les secteurs des infrastructures essentielles et qui sont organisées autour de résultats particuliers. Le noyau du cadre comprend quatre types d'éléments : les fonctions, les catégories, les sous-catégories et les références informatives (Cadre de sécurité du NIST, 2020).
- u) **Profil du cadre** (« profil ») : Résultats fondés sur les besoins opérationnels qu'une organisation a sélectionnés dans les catégories et sous-catégories du cadre. Le profil peut être défini comme l'harmonisation de normes, de lignes directrices et de pratiques au noyau du cadre dans un cas de mise en œuvre particulier. Les profils peuvent servir à relever les occasions d'améliorer la cybersécurité en comparant un profil « **actuel** » (l'état présent) et un profil « **cible** » (l'état futur). Pour créer un profil, une organisation peut passer en revue toutes les catégories et sous-catégories et, selon les facteurs liés à ses activités ou à sa mission et les résultats d'une évaluation des risques, déterminer lesquelles sont les plus importantes; des catégories et sous-catégories peuvent être ajoutées au besoin pour répondre aux risques de l'organisation. Le **profil actuel** peut alors servir à appuyer la définition des priorités et la mesure des progrès accomplis vers l'atteinte du **profil cible**, tout en tenant compte d'autres besoins opérationnels, notamment la rentabilité et l'innovation. Les profils peuvent aider à réaliser des auto-évaluations et à communiquer au sein d'une organisation ou entre organisations (Cadre de sécurité du NIST, 2020).
- v) **Risque** : Évaluation de la mesure dans laquelle une entité est menacée par une circonstance ou un événement potentiel, qui dépend généralement : (i) des effets négatifs qui surviendraient si la circonstance ou l'événement se produisait et (ii) de la probabilité d'occurrence (Cadre de sécurité du NIST, 2020).
- w) **Sous-catégorie** : Subdivision d'une catégorie en résultats particuliers d'activités techniques ou de gestion. Entre autres exemples de sous-catégories, citons « Les systèmes d'information externes sont catalogués », « Les données à l'arrêt sont protégées » et « Les notifications provenant des systèmes de détection font l'objet d'une enquête » (Cadre de sécurité du NIST, 2020).
- x) **Système de gestion de la circulation (SGC)** : Ce domaine concerne la gestion des déplacements de tous les types de véhicules, de voyageurs et de piétons sur l'ensemble du réseau de transport. Il s'occupe de la collecte, de la diffusion et du traitement de l'information pour le système de transport de surface. Il couvre à la fois les activités de surveillance et de contrôle automatisées, ainsi que les processus décisionnels (automatisés et manuels) qui traitent les incidents et autres perturbations en temps réel sur le réseau de transport, ainsi que la gestion de la demande de transport selon les besoins pour maintenir la mobilité globale (ARC-IT, 2020). Le SGC comprend le centre de gestion de la circulation, les communications centre à terrain, les systèmes de signalisation routière, les systèmes de transport intelligents, les systèmes de communication véhicule à infrastructure (V2I), les systèmes de communication infrastructure à autres, la télévision en circuit fermé, les contrôleurs et les boîtiers de signalisation routière, les panneaux à messages variables, les unités en bord de route, les systèmes de pesage en marche, les systèmes d'information sur la météo routière, les unités de traitement et de détection à distance, d'autres dispositifs adressables par IP et les réseaux de communication sur le terrain (National Cooperative Highway Research Program (NCHRP) Project 03-127 du Transportation Research Board (TRB), 2020).
- y) **Systèmes de transport intelligents (STI)** : Système qui se définit comme l'électronique, les communications ou le traitement de l'information dans les infrastructures de transport, intégré ou distinct, qui vise à améliorer la sécurité des transports et la mobilité et à accroître la productivité. Les systèmes de transport intelligents (STI) englobent un large éventail de technologies de

l'information et de technologies électroniques basées sur des communications sans fil ou filaires (ARC-IT, 2020).

- z) **Technologie de l'information (TI)** : Technologie consistant au développement, à la maintenance et à l'utilisation des systèmes, logiciels et réseaux informatiques aux fins du traitement et de la distribution des données.
- aa) **Technologie opérationnelle** : Matériel et logiciels qui détectent ou provoquent un changement par la surveillance ou le contrôle directs de l'équipement industriel, des biens, des processus et des événements.
- bb) **The Architecture Reference for Cooperative and Intelligent Transportation – ARC-IT** : ARC-IT fournit un cadre commun pour la planification, la définition et l'intégration des systèmes de transport intelligents. Ce produit mature reflète la contribution d'un large échantillon du milieu des STI (praticiens des transports, ingénieurs système, concepteurs de systèmes, spécialistes en technologie, experts-conseils, etc.).
- cc) **Unité de bord** : Dispositif V2X installé sur un véhicule et utilisé pour transmettre et recevoir différents messages à destination et en provenance d'autres dispositifs connectés (autres unités de bord ou unités en bord de route). Parmi les types de messages et les applications pris en charge par ce dispositif figurent les messages de sécurité des véhicules utilisés pour échanger de l'information sur les mouvements dynamiques de chaque véhicule à des fins de coordination et de sécurité (ARC-IT, 2020).
- dd) **Unité en bord de route** : Dispositif V2X connecté qui ne peut fonctionner qu'à partir d'une position fixe (qui peut en fait être une installation permanente ou un équipement temporaire apporté sur place pour la période associée à un incident, à la construction d'une route ou à un autre événement). Certaines peuvent être connectées à d'autres nœuds ou à Internet (ARC-IT, 2020).
- ee) **Véhicule connecté** : Véhicule contenant une unité de bord ou un dispositif de sécurité après-vente (ARC-IT, 2020).
- ff) **Véhicules automatisés** : Les véhicules automatisés utilisent des technologies de bord (p. ex. des caméras, des capteurs, le positionnement, des contrôleurs intelligents et, dans certains cas, la connectivité) pour naviguer tout en prenant le contrôle de certaines fonctions de conduite, comme le freinage, la direction et l'accélération. Les données des véhicules connectés permettent d'élargir la connaissance de la situation des véhicules automatisés au-delà de la portée limitée, de la visibilité directe et de la fiabilité de leurs capteurs de bord, pour offrir une plus grande assurance dans les situations où un système uniquement automatisé pourrait ne pas être fiable (ARC-IT, 2020).

Annexe B – Références

- a) Analyse factorielle du risque informationnel (FAIR), FAIR Institute (en anglais seulement)
- b) Cadre pour l'amélioration de la cybersécurité des infrastructures essentielles, version 1.1 (ou une version plus récente, en anglais seulement), NIST (comprend également les références faites à d'autres normes dans le cadre)
- c) Cybersecurity and Intelligent Transportation Systems: A Best Practice Guide, Département des Transports des États-Unis (en anglais seulement)
- d) Cybersecurity Capability Maturity Model (C2M2), Département de l'Énergie des États-Unis (en anglais seulement)
 - I. Cybersecurity Capability Maturity Model (C2M2) Facilitator Guide, version 1.1a (ou la version la plus récente) (en anglais seulement)
 - II. Cybersecurity Capability Maturity Model (C2M2), version 1.1 (ou la version la plus récente) (en anglais seulement)
 - III. Energy Sector Cybersecurity Framework Implementation Guidance (en anglais seulement)
- e) *Cybersecurity Framework*, version 1.1, Manufacturing Profile, révision 1), National Institute of Standards and Technology (NIST). Documents complémentaires :
 - I. *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance* (en anglais seulement)
 - II. *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case* (en anglais seulement)
 - III. *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case* (en anglais seulement)
- f) Cybersecurity Maturity Model Certification, Secrétaire à la défense pour l'acquisition et le maintien en puissance, Département de la défense des États-Unis (en anglais seulement)
- g) National Cooperative Highway Research Program (NCHRP) Project 03-127 - *Cybersecurity of Transportation Management Systems*, Transportation Research Board (TRB) [en anglais seulement], y compris :
 - I. *Task 1 - Cybersecurity Literature Review And Efforts Report*
 - II. *Web guidance tool*, accessible à l'adresse <https://cyberguidance.transportationops.org>
- h) *Cybersecurity Risk Management web-based Guidance Tool*, NCHRP, TRB (en anglais seulement)
- i) *Developing a Physical and Cyber Security Primer for Transportation Agencies*, NCHRP, TRB (en anglais seulement)
- j) Famille des normes ISO/IEC 27000 Systèmes de management de la sécurité de l'information, Organisation internationale de normalisation, qui comprend :
 - I. ISO/IEC 27000 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire
 - II. ISO/IEC 27002 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
 - III. ISO/IEC 27005 Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information
 - IV. ISO/IEC 27001 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- q) ISO/IEC/IEEE 15288:2015 Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système
- r) NIST, Security Assurance Levels: A Vector Approach to Describing Security Requirements, James D. Gilsinn, 2010 (en anglais seulement)

- s) NIST SP 800-160
 - I. Volume 1 : Ingénierie des systèmes et du logiciel – Considérations relatives à une approche multidisciplinaire pour l'ingénierie de systèmes sécuritaires (en anglais seulement)
 - II. Volume 2 : Ingénierie des systèmes et du logiciel – Processus du cycle de vie du système (en anglais seulement)
- k) Open Security Controls Assessment Language (OSCAL), NIST (en anglais seulement)
- l) Risk Management Framework for Information Systems and Organizations, publication spéciale 800-37, NIST (en anglais seulement)
- m) Security 101: A Physical and Cybersecurity Primer for Transportation Agencies, National Cooperative Highway Research Program, Transportation Research Board (en anglais seulement)
- n) Security Assurance Levels: A Vector Approach to Describing Security Requirements, paper publication, NIST (en anglais seulement)
- t) The Architecture Reference for Cooperative and Intelligent Transportation (en anglais seulement)
- o) The Cyber Resilience Review (en anglais seulement), version de février 2016, département américain de la Sécurité intérieure, qui comprend :
 - I. Cyber Resilience Review, **Method Description and User Guide** (en anglais seulement)
 - II. Cyber Resilience Review, **NIST Framework Crosswalk** (en anglais seulement)
 - III. Cyber Resilience Review, **Question Set with Guidance** (en anglais seulement)
 - IV. Cyber Resilience Review, **Self-Assessment Package** (en anglais seulement)
- u) The Purdue model for Industrial control systems, Industrial Cybersecurity, Pascal Ackerman, 2017 (en anglais seulement)
- p) US Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Evaluation Tool (CSET) [en anglais seulement]

Annexe C – Résumé des travaux connexes

- **Conseil des technologies de l'information et des communications (CTIC) – *Developing Cyber Talent for Canadian Critical Infrastructure – Road Transportation*** (<https://www.ictc-ctic.ca/developing-cyber-talent-canadian-critical-infrastructure-road-transportation/>, en anglais seulement). Ce rapport se penche sur les besoins des administrations routières canadiennes en main-d'œuvre spécialisée en cybersécurité. L'étude comporte une analyse des compétences essentielles et met en lumière la nécessité d'adopter une approche globale pour relever les défis liés au recrutement de la main-d'œuvre et au perfectionnement professionnel dans le secteur du transport routier.
- **CSET, CISA, département de la Sécurité intérieure des États-Unis** (<https://us-cert.cisa.gov/ics/Assessments>, en anglais seulement). Le CSET, outil basé sur le Web, aide les propriétaires et les exploitants d'infrastructures à s'autoévaluer par rapport à de nombreuses normes de cybersécurité applicables aux infrastructures essentielles.
- **CyberKit 1.0, Association des fabricants de pièces d'automobile du Canada** (<https://apma.ca/apma-cyberkit-1-0-2/>, en anglais seulement). La cybersécurité dans les secteurs automobile et manufacturier revêt toujours plus d'importance alors que l'industrie numérise la production. L'écosystème industriel est de plus en plus relié à l'Internet et à d'autres systèmes techniques et industries. Les systèmes électroniques des véhicules modernes sont fabriqués à partir de composants fournis par la multitude de distributeurs de nombreux fournisseurs qui n'ont que peu ou pas de normes de cybersécurité communes à respecter et prennent peu de dispositions relatives à la confidentialité ou à la sécurité dans leurs usines de fabrication. À l'heure actuelle, la cybersécurité de la chaîne d'approvisionnement des véhicules est extrêmement poreuse. Chaque fournisseur et chaque composant électronique sont un point de vulnérabilité potentiel. Les connaissances et l'expertise du comité sur la cybersécurité de l'Association des fabricants de pièces d'automobile du Canada (AFPAC) ont été mises à profit pour créer le **CyberKit 1.0**, qui sert à tous les fabricants de feuille de route globale pour implanter la cybersécurité dans leur milieu de travail ou revoir leurs activités de cybersécurité. Le **CyberKit 1.0** propose une approche structurée pour mettre au point un programme de gouvernance cybernétique complet dans une organisation, en commençant par désigner les responsables de la cybersécurité au sein de l'organisation. Sont ensuite présentés les méthodes d'évaluation des menaces et des risques et les cadres de gouvernance cybernétique, comme les normes ISO 21434 à venir et le cadre de cybersécurité du NIST, qui peuvent être mis en place pour évaluer les risques et protéger une organisation contre les risques cybernétiques.
- **Cybersecurity for Intelligent Transportation Systems, Joint Program Office (ITS JPO)** (https://www.its.dot.gov/about/its_jpo.htm, en anglais seulement). L'ITS JPO a tissé un partenariat avec les sites pilotes de véhicules connectés afin d'adapter le cadre de cybersécurité du NIST aux environnements de véhicules connectés. Ils ont apporté l'expertise d'entreprises publiques et privées en matière d'exigences des utilisateurs et de contre-mesures indispensables à l'établissement des directives du cadre de cybersécurité pour l'environnement des véhicules connectés. Ce projet visait à l'origine à élaborer un profil cible du NIST pour les sites pilotes de véhicules connectés et autonomes, mais il est actuellement étendu pour élaborer un profil cible du NIST pour les systèmes de transport intelligents.
- **Cybersecurity Resilience Review (CRR), CISA, département de la Sécurité intérieure des États-Unis** (<https://us-cert.cisa.gov/resources/assessments>, en anglais seulement). Le CRR est

un outil d'auto-évaluation de la cybersécurité pour les infrastructures essentielles. Sécurité publique Canada a produit une version canadienne du CRR.

- **Lignes directrices sur la cybersécurité des véhicules au Canada** (<https://tc.canada.ca/fr/transport-routier/technologies-novatrices/vehicules-automatisees-connectees/securite-vehicules-connectees-automatisees-ce-qu-il-faut-savoir>). Les lignes directrices sur la cybersécurité des véhicules au Canada ont été élaborées en étroite collaboration avec des partenaires du gouvernement et de l'industrie. Ces lignes directrices fournissent un ensemble de principes directeurs neutres sur le plan technologique afin d'appuyer l'industrie pour renforcer la cyberrésilience des véhicules, et constituent un pas important vers l'évolution de la situation de la cybersécurité des véhicules au Canada. Le projet décrit dans le présent énoncé de travail sera complémentaire à ces lignes directrices et portera principalement sur l'infrastructure.
- **Penetration Testing: Best Practice Guide, département des Transports des États-Unis** (https://rosap.ntl.bts.gov/view/dot/42461/dot_42461_DS1.pdf, en anglais seulement). Les directives fournissent aux agences de transport des municipalités et des États américains un modèle d'énoncé des travaux pour l'obtention de services d'essai de pénétration.
- **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>, en anglais seulement). Cette recherche visait à élaborer des directives à l'intention des agences de transport des États et des municipalités sur la réduction des risques de cyberattaques du côté extérieur des systèmes de gestion du trafic (ce qui comprend les systèmes de signalisation routière, les systèmes de transport intelligents, les systèmes de communication entre les véhicules et l'infrastructure et les systèmes de télévision en circuit fermé) et, accessoirement, sur les façons de réagir à une attaque.

ANNEXE « B »

BASE DE PAIEMENT

Le paiement des services rendus sera effectué lorsque les produits livrables auront été reçus et acceptés par le représentant ministériel et après la remise de factures détaillées.

Tous les paiements seront versés seulement si TC est satisfait des produits livrables.

Voici le calendrier selon lequel les paiements seront versés chaque exercice financier conformément au contrat :

Exercice financier 2020-2021 – de la date d'attribution au 31 mars 2021

Paieement	Livrable	Description	Prix fixe
1	1	À l'achèvement et à l'approbation du livrable 1 Tâche 5.1 – Plan de gestion du projet	<u>[Insérer lors de l'attribution du marché] \$</u> (TPS/TVH en sus)
Prix total fixe			<u>[Insérer lors de l'attribution du marché] \$</u> (TPS/TVH en sus)

Exercice financier 2021-2022 – Du 1^{er} avril 2021 au 31 mars 2022 :

Paieement	Livrable	Description	Prix fixe
2	2	À l'achèvement et à l'approbation du livrable 2 Livrables des tâches 5.2.2 à 5.2.5 – versions provisoires : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ.	<u>[Insérer lors de l'attribution du marché] \$</u> (TPS/TVH en sus)
3	3 et 4	À l'achèvement et à l'approbation des livrables 3 et 4 Livrables des tâches 5.2.2 à 5.2.5 – versions révisées : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ. Rapport sur la résolution des commentaires. Livrables des tâches 5.2.2 à 5.2.5 – versions définitives : plan de la boîte à outils, abécédaire de la	<u>[Insérer lors de l'attribution du marché] \$</u> (TPS/TVH en sus)

		cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ. Rapport sur la résolution des commentaires.	
4	5	À l'achèvement et à l'approbation du livrable 5 Livrables des tâches 5.2.6 et 5.2.7 – Six séances de formation virtuelle et webinaire enregistré.	[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)
5	6 à 11	À l'achèvement et à l'approbation des livrables 6 à 11 Livrables de la tâche 5.3.1 – document de conception et questionnaire. Boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3), guide de l'utilisateur (tâche 5.3.5), démonstration de la boîte à outils par webinaire, et les rapports sur la résolution des commentaires.	[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)
Prix total fixe			[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)

Exercice financier 2022-2023 – Du 1^{er} avril 2022 au 31 mars 2023

Paielement	Livrable	Description	Prix fixe
6	12 à 15	À l'achèvement et à l'approbation des livrables 12 à 15 Livrable de la tâche 5.4.1 – directives et les rapports sur la résolution des commentaires	[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)
7	16 à 18	À l'achèvement et à l'approbation des livrables 16 à 18 Tâche 5.5.1 – Ordres du jour et des diapositives de présentation pour les séances de consultation. Offre de trois séances de consultation de groupe aux intervenants et de 15 séances individuelles sur la boîte à outils (tâche 5.3) et l'orientation (tâche 5.4).	[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)
8	19	À l'achèvement et à l'approbation du livrable 19 Tâche 5.5.2 – Offre de services de soutien technique sur place et à distance à trois administrations	[Insérer lors de l'attribution du marché] \$ (TPS/TVH en sus)

		routières.	
9	20 à 21	À l'achèvement et à l'approbation des livrables 20 à 21 Tâche 5.5.3 - Résumé de la rétroaction obtenue lors des séances de consultation, des enseignements tirés de la mise en œuvre et du soutien ainsi que des changements proposés à la boîte à outils et aux documents d'orientation. Versions révisées de la boîte à outils et des directives.	<u>[Insérer lors de l'attribution du marché]</u> \$ (TPS/TVH en sus)
Prix total fixe			<u>[Insérer lors de l'attribution du marché]</u> \$ (TPS/TVH en sus)

Exercice financier 2023-2024 – Du 1^{er} avril 2023 au 31 mars 2024

Paiement	Livable	Description	Prix fixe
10	22 à 24	À l'achèvement et à l'approbation des livrables 22 à 24 Livrables des tâches 5.5.4.1 et 5.5.4.2 – ordres du jour, matériel de formation, diapositives de présentation, et rapports de résolution des commentaires.	<u>[Insérer lors de l'attribution du marché]</u> \$ (TPS/TVH en sus)
11	25	À l'achèvement et à l'approbation du livrable 25 Tâche 5.5.4.3 – Tenue de six séances de formation.	<u>[Insérer lors de l'attribution du marché]</u> \$ (TPS/TVH en sus)
Prix total fixe			_____ \$ (TPS/TVH en sus)

Services professionnels (autorisation de tâche)

L'entrepreneur sera payé pour les travaux précisés dans l'autorisation de tâches accordée, conformément aux taux horaires des tâches indiqués ci-après :

Tâche optionnelle 5.6.1 - Consultation supplémentaire, soutien technique et formation au besoin – Pour un prix journalier fixe de [\[insérer à l'attribution du contrat\]](#) \$ (TPS/TVH en sus)

Tâche optionnelle 5.6.2 – Analyse de la vulnérabilité de la cybersécurité (à l'exclusion des tests de pénétration) et conseils stratégiques au fur et à mesure des besoins. – Pour un prix journalier fixe de [\[insérer à l'attribution du contrat\]](#) \$ (TPS/TVH en sus)

Tâche optionnelle 5.6.3 – Essais de pénétration, analyse des vulnérabilités et identification des exploits des systèmes et de l'équipement, fournis au besoin. – Pour un prix journalier fixe de **[insérer à l'attribution du contrat]** \$ (TPS/TVH en sus)

Frais de déplacement et de subsistance autorisés pour les travaux

En ce qui concerne les déplacements éventuels à effectuer, décrits à l'annexe A de l'Énoncé des travaux, l'entrepreneur se verra payer les frais autorisés de déplacement et de subsistance qu'il a raisonnablement et dûment engagés pour accomplir les travaux à exécuter, à livrer ou à fournir au prix coûtant, sans aucune indemnité pour le profit et les frais administratifs généraux, conformément aux indemnités relatives aux repas et à l'utilisation d'un véhicule privé qui sont précisés aux appendices B, C et D de la [Directive sur les voyages du Conseil national mixte](#); à l'extérieur de la région de la capitale nationale (RCN) définie dans la [Loi sur la capitale nationale \(L.R.C. \[1985\], ch. N-4\)](#), accessible sur le site Web de Justice (<http://laws-lois.justice.gc.ca/fra/acts/N-4/page-9.html#docCont>). Tout déplacement doit être approuvé au préalable par le chargé de projet.

Le gouvernement du Canada n'acceptera aucuns frais de déplacement et de subsistance que l'entrepreneur pourrait devoir engager pour le transfert des ressources nécessaires afin de s'acquitter de ses obligations contractuelles » et selon les autres dispositions de la Directive qui font référence aux « voyageurs » plutôt qu'à celles qui font référence aux « employés ».

Le gouvernement du Canada n'acceptera aucuns frais de déplacement et de subsistance engagés par l'entrepreneur à cause d'un déménagement des ressources nécessaires pour respecter les modalités du présent contrat. »

Les frais de déplacement et de subsistance autorisés seront remboursés sur présentation d'un état détaillé des coûts accompagné des reçus appropriés. Tous les paiements sont assujettis à un audit du gouvernement.

N° de l'invitation - Sollicitation No.

T8080-200405

N° de réf. du client - Client Ref. No.

N° de la modif - Amd. No.

File No. - N° du dossier

Id de l'acheteur - Buyer ID

Kristen Scott

N° CCC / CCC No./ N° VME - FMS

ANNEXE « C »

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

****CI-JOINT COMME DOCUMENT DISTINCT**

ANNEXE « D »

PROCESSUS D'ÉVALUATION

- a) Les soumissions seront évaluées en fonction de toutes les exigences figurant dans la demande de soumissions, y compris les critères d'évaluation technique et financière.
- b) Un comité d'évaluation composé de représentants du Canada évaluera les soumissions.

Évaluation technique

Critères techniques obligatoires

Les exigences obligatoires seront évaluées selon qu'elles sont jugées satisfaites ou non.

Les propositions qui ne satisfont pas aux exigences seront jugées non recevables et seront écartées.

Remarque : TC peut décider de mettre fin à l'évaluation de toute proposition dès le premier constat de non-respect d'une exigence obligatoire ou dès le premier constat qu'une proposition n'obtient pas une note minimale à l'égard d'une exigence cotée.

Un comité d'évaluation composé de représentants du gouvernement du Canada évaluera les propositions.

Le comité d'évaluation se réserve le droit d'effectuer les démarches suivantes (mais n'est pas tenue de le faire) :

- a) demander des précisions ou vérifier la totalité ou une partie des renseignements fournis par le soumissionnaire à l'égard de la présente demande de propositions;
- b) communiquer avec l'une ou l'ensemble des personnes citées en référence; ces personnes doivent être consultées uniquement pour attester l'exactitude des renseignements figurant dans la soumission.

Critères obligatoires

Les propositions seront évaluées conformément aux critères d'évaluation obligatoires indiqués aux présentes. Les propositions présentées par les soumissionnaires doivent démontrer clairement qu'elles répondent à toutes les exigences obligatoires pour qu'elles soient retenues aux fins d'une évaluation subséquente. Les propositions qui ne satisfont pas aux critères obligatoires ne seront pas retenues.

Tout sommaire de projet fourni par le soumissionnaire pour prouver qu'il satisfait aux exigences obligatoires ou cotées relatives à l'expérience doit comprendre :

1. Une description du projet et de la portée des services rendus, des livrables et des résultats;
2. La valeur du projet;
3. S'il y a lieu, le numéro de référence de la demande de soumissions ou l'avis d'adjudication, accompagné d'un lien vers le site du gouvernement où sont publiés les appels d'offres;
4. L'ampleur du projet (taille de l'organisation cliente, le cas échéant);
5. Les dates et la durée du projet (inscrire les mois et années de participation, ainsi que les dates de début et d'achèvement des travaux);

6. Une brève description du rôle de la ou des ressources proposées dans le projet;
7. Le nom de l'organisation cliente (s'il peut être donné);
8. La confirmation que les services rendus et les livrables ont satisfait aux attentes du client en termes de délai, de budget et de qualité du travail.

Le soumissionnaire peut utiliser un sommaire de projet individuel afin de répondre à un ou plusieurs critères obligatoires ou cotés. Le soumissionnaire peut choisir de fournir des sommaires de projet au début de sa proposition et de les citer en référence pour répondre à chacun des critères, tout en apportant des précisions supplémentaires au besoin. Le soumissionnaire évitera ainsi de répéter les mêmes renseignements à plusieurs reprises.

Le soumissionnaire doit joindre le tableau ci-après à sa proposition et indiquer que celle-ci satisfait aux critères obligatoires. Il doit indiquer le numéro de page et la section de la proposition où se trouvent les renseignements permettant de vérifier s'il satisfait aux critères.

Tableau 1 : Critères obligatoires

N°	Critères obligatoires	Critère satisfait (✓)	N° de page dans la proposition
O1	<p>Au cours des dix (10) dernières années, les ressources proposées du soumissionnaire doivent avoir, collectivement, réalisé trois (3) projets ayant trait à la réalisation d'évaluations de la cybersécurité sur des systèmes d'infrastructures essentielles (p. ex. le secteur des transports, le secteur financier, le secteur de l'énergie) en employant des méthodes ou des normes reconnues, comme la norme ISO 27001, le cadre de cybersécurité du NIST ou d'autres normes de cybersécurité appropriées.</p> <p>Remarque : Cette exigence peut être démontrée par un total de trois projets réalisés par au moins une des ressources proposées. Si différentes ressources sont proposées, elles ne sont pas tenues d'avoir travaillé aux mêmes projets pour que ceux-ci soient pris en considération au titre de l'expérience. Cette exigence doit être démontrée au moyen de sommaires de projet, conformément aux exigences générales.</p>		
O2	<p>Le soumissionnaire doit joindre à sa proposition le curriculum vitæ (CV) détaillé de chacune des ressources proposées pour ce contrat et indiquer le rôle de chacune dans la réalisation du contrat.</p> <p>Le CV de chaque ressource proposée doit comprendre un résumé ou une description des projets antérieurs et de l'expérience professionnelle acquise au cours des dix (10) dernières années, en précisant le lieu de réalisation des travaux et la durée.</p>		

O3	<p>Le CV d'au moins une des ressources proposées doit prouver qu'elle possède l'expérience suivante :</p> <ul style="list-style-type: none"> • présenter des exposés devant de grands groupes d'intervenants (plus de 50 personnes); • chapeauter des groupes de travail techniques, des groupes de travail ou toute autre initiative de collaboration. 		
O4	<p>Le CV d'au moins une ressource proposée doit démontrer un minimum de cinq (5) ans* d'expérience dans la réalisation d'analyses de la vulnérabilité et d'essais de pénétration sur des systèmes d'infrastructure essentielle.</p> <p>Cette ressource doit être en mesure d'obtenir une cote de sécurité de niveau secret (niveau II) du gouvernement du Canada, obligatoire pour les tâches optionnelles 5.6.2 et 5.6.3, tel qu'indiqué dans la section 16.</p> <p>Cette exigence peut être satisfaite par des sous-traitants qui possèdent l'expérience et la cote de sécurité demandées.</p> <p>* L'expérience ne doit pas nécessairement avoir été acquise au cours de cinq (5) années consécutives.</p>		
O5	<p>Le soumissionnaire doit proposer un gestionnaire de projet* qui possède au moins cinq (5) ans** d'expérience en gestion de projet.</p> <p>Son CV doit attester de cette expérience.</p> <p>* Les responsabilités du gestionnaire de projet sont décrites au point 18.</p> <p>** L'expérience ne doit pas nécessairement avoir été acquise au cours de cinq (5) années consécutives.</p>		
O6	<p>Le soumissionnaire doit joindre un plan de projet provisoire et une description de l'approche proposée pour répondre aux exigences de la tâche et gérer les risques potentiels du projet.</p> <p>Le plan du projet doit préciser les cibles provisoires hebdomadaires pour toutes les tâches et tous les produits livrables ainsi que la répartition du temps de chaque ressource du projet en jours-personnes.</p> <p>Le plan du projet doit décrire brièvement le rôle de chaque ressource dans le projet.</p>		
O7	<p>Le soumissionnaire doit avoir accès à une installation ou à un laboratoire pour effectuer les essais de pénétration liés à la tâche 5.6.3 et doit fournir une description du plan qu'il prévoit suivre pour effectuer le travail dans le cadre de cette option du contrat avec des</p>		

N° de l'invitation - Sollicitation No.

T8080-200405

N° de réf. du client - Client Ref. No.

N° de la modif - Amd. No.

File No. - N° du dossier

Id de l'acheteur - Buyer ID

Kristen Scott

N° CCC / CCC No./ N° VME - FMS

	ressources qui satisfont à l'exigence obligatoire O4.		
O8	La partie technique de l'offre ne doit pas dépasser 100 pages (sans compter le titre, la table des matières, le plan du projet et les CV).		

Exigences techniques

Critères techniques cotés

Les soumissions qui satisfont à tous les critères obligatoires seront évaluées et notées selon les précisions données ci-après.

Les soumissions doivent obtenir une note globale minimale de 65 %. Les soumissions qui ne répondent pas à cette exigence seront déclarées non recevables. Chaque critère technique coté doit être traité séparément.

Nous conseillons aux soumissionnaires de répondre dans l'ordre qui suit et de façon détaillée pour permettre une évaluation exhaustive. L'évaluation se fondera seulement sur les renseignements donnés dans la proposition. Le comité d'évaluation pourra vérifier les renseignements donnés et demander des précisions.

Les éléments de la proposition du soumissionnaire se verront attribuer un pourcentage de points, de la manière suivante :

Tableau 2: Critères techniques cotés

Critères cotés	Cotation numérique	Pointage maximum	N° de page dans la proposition
C1. Qualité du plan de projet et description de l'approche proposée			
Le soumissionnaire doit joindre son plan de projet provisoire pour répondre aux exigences des tâches 5.1 à 5.5 conformément au calendrier du point 6. Le soumissionnaire doit également joindre une description des ressources et de l'approche qu'il propose pour les travaux prévus dans le cadre des options du contrat, conformément à la tâche 5.6. Le plan du projet doit préciser les cibles provisoires hebdomadaires pour toutes les tâches et tous les produits livrables, ainsi que la répartition du temps de chaque ressource du projet en jours-personnes. Le plan de projet doit également comprendre une	Aucun plan = 0 point. Plan inadéquat qui ne détaille pas ou ne précise pas de manière efficace la répartition des tâches entre les ressources du projet et la façon d'arriver aux résultats attendus, et qui présente des lacunes majeures en ce qui concerne les renseignements = 4 points. Plan inadéquat qui ne détaille pas ou ne précise pas de manière efficace la répartition des tâches entre les ressources du projet et la façon d'arriver aux résultats attendus, et qui présente d'importantes lacunes en ce qui concerne les renseignements = 8 points. Plan adéquat qui fournit suffisamment de détails sur la répartition des tâches entre les ressources du projet et sur la façon réaliste d'arriver aux	20	

<p>description de l'approche proposée pour répondre aux exigences de la tâche (ce qui comprend l'élaboration de la boîte à outils et des documents d'orientation sur la cybersécurité) et gérer les risques potentiels du projet. Dans son plan de projet, le soumissionnaire doit supposer que la date d'attribution du contrat est le 1^{er} février 2021.</p>	<p>résultats attendus, et qui présente certaines lacunes en ce qui concerne les renseignements = 12 points.</p> <p>Bon plan qui fournit suffisamment de détails sur la répartition des tâches entre les ressources du projet et sur la façon réaliste d'arriver aux résultats attendus, et qui présente quelques lacunes mineures en ce qui concerne les renseignements = 16 points.</p> <p>Excellent plan exhaustif qui fournit suffisamment de détails sur la répartition des tâches entre les ressources du projet et sur la façon réaliste d'arriver aux résultats attendus; des lacunes très mineures en ce qui concerne les renseignements = 20 points.</p>		
<p>C2. Expérience professionnelle dans la réalisation d'évaluations de la cybersécurité ou de vérifications sur des systèmes d'infrastructures essentielles ou dans l'encadrement d'une organisation lors de celles-ci</p>			
<p>Au moins une des ressources proposées possède de l'expérience dans la réalisation d'évaluations de la cybersécurité ou de vérifications sur des systèmes d'infrastructures essentielles ou dans l'encadrement d'une organisation lors de celles-ci (conformément au cadre de cybersécurité du NIST, à la norme ISO 27001 ou à un autre cadre réputé sur les systèmes d'infrastructures essentielles, comme le secteur des transports, le secteur financier, le secteur de l'énergie).</p> <p>Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au</p>	<p>Étendue de l'expérience (maximum de 5 points) : 1 point par projet d'évaluation pertinent réalisé au cours des dix (10) dernières années qui visait un client d'au moins 5 000 employés ou était pluriannuel; 0,5 point par autre projet pertinent réalisé au cours des dix (10) dernières années. Pour qu'un exemple de projet puisse être considéré comme étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux.</p> <p>Pertinence et portée de l'expérience (maximum de 5 points) : Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont</p>	<p>10</p>	

<p>point « Exigences générales », et détailler :</p> <ul style="list-style-type: none">• le rôle de la ou des ressources proposées pour chaque exemple de projet;• la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux.	<p>pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 2 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 4 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 5 points.</p>		
--	--	--	--

<p>C3. Expérience professionnelle dans l'élaboration de matériel et de programmes de formation, ainsi que dans la direction, l'organisation et la tenue d'activités de formation sur la cybersécurité à l'échelle de l'entreprise</p>			
<p>Au moins l'une des ressources proposées possède de l'expérience professionnelle dans l'élaboration de matériel et de programmes de formation, ainsi que dans la direction, l'organisation et la tenue d'activités de formation sur la cybersécurité à l'échelle de l'entreprise.</p> <p>Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none"> le rôle de la ou des ressources proposées pour chaque exemple de projet; la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux. 	<p>Étendue de l'expérience (maximum de 5 points) : 1 point par projet de programme de formation pertinent réalisé au cours des dix (10) dernières années qui visait au moins 100 employés ou était pluriannuel; 0,5 point par autre projet pertinent réalisé au cours des dix (10) dernières années. Pour qu'un exemple de projet puisse être considéré comme étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux. Pertinence et portée de l'expérience (maximum de points) : Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point. Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 2 points. Le rôle et l'expérience de la ou</p>	10	

	<p>des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 4 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 5 points.</p>		
<p>C4. Expérience professionnelle dans l'élaboration d'outils d'évaluation de la cybersécurité et de documents d'orientation pour des systèmes d'infrastructures essentielles</p>			
<p>Au moins une des ressources proposées possède de l'expérience dans l'élaboration de questionnaires d'évaluation de la cybersécurité interactifs (qui permettent de recueillir et d'analyser les commentaires des utilisateurs) ou d'autres outils semblables à ceux décrits dans l'énoncé des travaux pour des systèmes d'infrastructures essentielles, ainsi que dans la préparation de documents d'orientation connexes (comme des guides de</p>	<p>Étendue de l'expérience (maximum de 5 points) : 1 point par projet pertinent réalisé au cours des dix (10) dernières années comprenant un outil d'évaluation de la cybersécurité et des documents d'orientation; 0,5 point par projet pertinent réalisé au cours des dix (10) dernières années comprenant uniquement un outil d'évaluation de la cybersécurité ou des documents d'orientation pour la réalisation d'une évaluation de la cybersécurité. Pour qu'un exemple de projet puisse être considéré comme</p>	<p>15</p>	

<p>l'utilisateur). Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none">• le rôle de la ou des ressources proposées pour chaque exemple de projet;• la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux.	<p>étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux.</p> <p>Pertinence et portée de l'expérience (maximum de 10 points) : Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 6 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du</p>		
---	--	--	--

	<p>projet = 8 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 10 points.</p>		
<p>C5. Expérience de travail dans la préparation des produits livrables pour des gouvernements fédéral, provinciaux ou territoriaux au Canada ou des gouvernements d'États américains sous la forme de présentations ou de rapports</p>			
<p>Au moins l'une des ressources proposées possède de l'expérience dans la préparation des produits livrables pour des gouvernements fédéral, provinciaux ou territoriaux du Canada ou des gouvernements d'États américains sous la forme de présentations ou de rapports.</p> <p>Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none"> le rôle de la ou des ressources proposées pour chaque exemple de projet; la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des 	<p>Étendue de l'expérience (maximum de 5 points) : 1 point par projet pertinent. Pour qu'un exemple de projet puisse être considéré comme étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux.</p> <p>Pertinence et portée de l'expérience (maximum de 5 points) : Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet</p>	10	

travaux.	<p>= 2 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 4 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 5 points.</p>		
<p>C6. Expérience professionnelle dans la réalisation d'analyses techniques de vulnérabilité de la cybersécurité et d'essais de pénétration sur des systèmes ou de l'équipement de contrôle industriels</p>			
<p>Au moins l'une des ressources proposées possède de l'expérience dans la réalisation d'analyses pratiques de la vulnérabilité de la cybersécurité et d'essais de pénétration sur des systèmes ou de l'équipement de contrôle industriels :</p> <p>a) Collecte et examen de renseignements pour caractériser l'équipement et préparer les essais de</p>	<p>Étendue de l'expérience (maximum de 5 points) : 1 point par projet pertinent réalisé au cours des dix (10) dernières années. Pour qu'un exemple de projet puisse être considéré comme étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux.</p> <p>Pertinence et portée de</p>	10	

<p>vulnérabilité</p> <p>b) Configuration de sous-systèmes de véhicules et de systèmes de gestion des transports en laboratoire pour préparer les essais</p> <p>c) Réalisation d'essais sur le terrain</p> <p>d) Mise à l'essai des mesures d'atténuation recommandées</p> <p>e) Évaluation de l'applicabilité et des lacunes des normes et des protocoles de cybersécurité</p> <p>f) Élaboration de procédures pour les essais de cybersécurité</p> <p>g) Application des normes relatives aux essais de cybersécurité (par exemple, Open Web Application Security Project).</p> <p>h) Utiliser les logiciels et les cadres existants pour les essais de cybersécurité (par exemple, des scanners d'applications Web comme OWASP Zap, des scanners de vulnérabilité, logiciels de criminalistique numérique).</p> <p>Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none"> le rôle de la ou des 	<p>l'expérience (maximum de 5 points) :</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 2 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 4 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux;</p>		
--	--	--	--

<p>ressources proposées pour chaque exemple de projet;</p> <ul style="list-style-type: none"> la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux. 	<p>l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 5 points.</p>		
<p>C7. Expérience de travail sur des projets de cybersécurité dans le secteur des transports, qui touchaient notamment à des systèmes de gestion de transports, à des systèmes de transport intelligents ou à des véhicules connectés et automatisés</p>			
<p>Au moins une des ressources proposées possède de l'expérience de travail sur des projets de cybersécurité dans le secteur des transports.</p> <p>Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none"> le rôle de la ou des ressources proposées pour chaque exemple de projet; la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux. 	<p>Étendue de l'expérience (maximum de 10 points) : 0,5 point par projet pertinent dans le secteur des transports; 1,5 point supplémentaire par projet pertinent qui touchait spécifiquement à des systèmes de gestion de transports, à des systèmes de transport intelligents ou à des véhicules connectés et automatisés. Pour qu'un exemple de projet puisse être considéré comme étant pertinent, le soumissionnaire doit expliquer clairement dans quelle mesure l'expérience de la ou des ressources proposées s'applique au présent énoncé des travaux.</p> <p>Pertinence et portée de l'expérience (maximum de 10 points) : Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de</p>	<p>20</p>	

	<p>répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 6 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 8 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et appliquée à toutes les exigences du projet, voire de les dépasser = 10 points.</p>		
<p align="center">C8. Expérience de travail dans la direction de groupes de travail, de consultations ou de toute autre initiative de collaboration multilatérale</p>			
<p>Au moins l'une des ressources proposées possède de l'expérience</p>	<p>Pertinence et portée de l'expérience (maximum de 5 points) :</p>	<p align="center">5</p>	

<p>dans la direction de groupes de travail, de consultations ou de toute autre initiative de collaboration multilatérale. Cette expérience doit être démontrée au moyen d'un texte descriptif faisant référence aux sommaires de projet, conformément au point « Exigences générales », et détailler :</p> <ul style="list-style-type: none">• le rôle de la ou des ressources proposées pour chaque exemple de projet;• la mesure dans laquelle l'expérience de la ou des ressources proposées s'applique, est pertinente pour le rôle proposé et satisfait aux exigences de l'énoncé des travaux.	<p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas pertinents en ce qui concerne ce critère de l'énoncé des travaux; ou il n'y a pas suffisamment de détails pour prouver que l'expérience de travail peut être transférée et appliquée au projet afin de répondre aux exigences de celui-ci = 0 point.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits ne sont pas suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à quelques exigences du projet = 2 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à un grand nombre des exigences du projet = 3 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut être transférée et appliquée à la plupart des exigences du projet = 4 points.</p> <p>Le rôle et l'expérience de la ou des ressources proposées dans les projets décrits sont suffisamment pertinents en ce qui concerne ce critère de l'énoncé des travaux; l'expérience décrite peut clairement être transférée et</p>		
--	--	--	--

N° de l'invitation - Sollicitation No.

T8080-200405

N° de réf. du client - Client Ref. No.

N° de la modif - Amd. No.

File No. - N° du dossier

Id de l'acheteur - Buyer ID

Kristen Scott

N° CCC / CCC No./ N° VME - FMS

	appliquée à toutes les exigences du projet, voire de les dépasser = 5 points		
TOTAL CRITÈRES COTÉS (Maximum 100 points) Note de passage (65% - 65 Points)			
Total Points			/100

ANNEXE «E »

BARÈME DE PRIX

Services professionnels et frais connexes

L'entrepreneur doit proposer un prix fixe tout inclus pour l'exécution des travaux décrits dans les tâches 5.1 à 5.5 de l'énoncé des travaux. De plus, l'entrepreneur doit présenter une ventilation du prix fixe tout inclus soumis, conformément au tableau A.

Tableau A – Proposition de coût pour les travaux de base

Livrable	Tâche associée	Description du livrable	Prix fixe évalué
1	5.1	Tâche 5.1 – Plan de gestion du projet.	_____ \$ (TPS/TVH en sus)
2	5.2	Livrables des tâches 5.2.2 à 5.2.5 – versions provisoires : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ.	_____ \$ (TPS/TVH en sus)
3	5.2	Livrables des tâches 5.2.2 à 5.2.5 – versions révisées : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ. Rapport sur la résolution des commentaires.	_____ \$ (TPS/TVH en sus)
4	5.2	Livrables des tâches 5.2.1 à 5.2.5 – versions définitives : plan de la boîte à outils, abécédaire de la cybersécurité dans les transports routiers, document d'information, diapositives de présentation et FAQ. Rapport sur la résolution des commentaires.	_____ \$ (TPS/TVH en sus)
5	5.2	Livrables des tâches 5.2.6 et 5.2.7 – Six séances de formation virtuelle et webinaire enregistré.	_____ \$ (TPS/TVH en sus)
6	5.3	Livrables de la tâche 5.3.1 – version provisoire : document de conception et questionnaire.	_____ \$ (TPS/TVH en sus)
7	5.3	Livrables de la tâche 5.3.1 – version révisée : document de conception et questionnaire.	_____ \$ (TPS/TVH en sus)
8	5.3	Livrables de la tâche 5.3.1 – version définitive : document de conception et questionnaire.	_____ \$ (TPS/TVH en sus)

Livrable	Tâche associée	Description du livrable	Prix fixe évalué
9	5.3	Prototype de boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3), version provisoire du guide de l'utilisateur (tâche 5.3.5), et démonstration de la boîte à outils par webinaire.	_____ \$ (TPS/TVH en sus)
10	5.3	Version révisée de la boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3) et du guide de l'utilisateur (tâche 5.3.5), démonstration de la boîte à outils par webinaire et résumé de la résolution des commentaires.	_____ \$ (TPS/TVH en sus)
11	5.3	Version définitive de la boîte à outils fonctionnelle (tâches 5.3.2 et 5.3.3) et du guide de l'utilisateur (tâche 5.3.5), démonstration de la boîte à outils par webinaire et résumé de la résolution des commentaires.	_____ \$ (TPS/TVH en sus)
12	5.4	Livrable de la tâche 5.4.1 – Aperçu des directives.	_____ \$ (TPS/TVH en sus)
13	5.4	Livrable de la tâche 5.4.1 – Version provisoire des directives.	_____ \$ (TPS/TVH en sus)
14	5.4	Livrables de la tâche 5.4.1 – version révisée des directives et du rapport sur la résolution des commentaires.	_____ \$ (TPS/TVH en sus)
15	5.4	Livrables de la tâche 5.4.1 – version définitive* des directives et du rapport sur la résolution des commentaires. *consultation préalable	_____ \$ (TPS/TVH en sus)
16	5.5	Tâche 5.5.1.1 – versions provisoires des ordres du jour et des diapositives de présentation pour les séances de consultation.	_____ \$ (TPS/TVH en sus)
17	5.5	Tâche 5.5.1.1 – versions définitives des ordres du jour et des diapositives de présentation pour les séances de consultation.	_____ \$ (TPS/TVH en sus)
18	5.5	Tâche 5.5.1 – Offre de trois séances de consultation de groupe aux intervenants et de 15 séances individuelles sur la boîte à outils (tâche 5.3) et l'orientation (tâche 5.4).	_____ \$ (TPS/TVH en sus)
19	5.5	Tâche 5.5.20 – Offre de services de soutien technique sur place et à distance à trois administrations routières.	_____ \$ (TPS/TVH en sus)
20	5.5	Tâche 5.5.3.1 – Résumé de la rétroaction obtenue lors des séances de consultation, des enseignements tirés de la mise en œuvre et du soutien ainsi que des changements proposés à la boîte à outils et aux documents d'orientation.	_____ \$ (TPS/TVH en sus)

Livrable	Tâche associée	Description du livrable	Prix fixe évalué
21	5.5	Tâche 5.5.3.2 – versions révisées de la boîte à outils et des directives.	_____ \$ (TPS/TVH en sus)
22	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions provisoires des ordres du jour, du matériel de formation et des diapositives de présentation.	_____ \$ (TPS/TVH en sus)
23	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions révisées des ordres du jour, du matériel de formation et des diapositives de présentation, et rapport de résolution des commentaires.	_____ \$ (TPS/TVH en sus)
24	5.5	Livrables des tâches 5.5.4.1 et 5.5.4.2 – versions définitives des ordres du jour, du matériel de formation et des diapositives de présentation, et rapport de résolution des commentaires.	_____ \$ (TPS/TVH en sus)
25	5.5	Tâche 5.5.4.3 – Tenue de six séances de formation.	_____ \$ (TPS/TVH en sus)
Prix fixe total évalué pour les travaux de base			_____ \$ (TPS/TVH en sus)

Services professionnels (autorisation de tâche)

L'entrepreneur doit proposer un tarif journalier pour chaque tâche optionnelle qui couvre le travail d'une ressource par jour de travail. Le travail optionnel ne peut être commencé et payé qu'après approbation et achèvement de l'autorisation de tâches pour la ou les tâches optionnelles en question. Veuillez noter que les tâches optionnelles peuvent être invoquées à tout moment pendant la durée du contrat, une fois que les exigences applicables à la cote de sécurité ont été satisfaites.

Tableau B – Proposition de coût pour les travaux optionnels

Tâche optionnelle	Tarif journalier (par jour-personne)
Tâche optionnelle 1 : Tâche 5.6.1 : Consultation supplémentaire, soutien technique et formation au besoin	_____ \$ par jour-personne (TPS/TVH en sus)

Tâche optionnelle	Tarif journalier (par jour-personne)
Tâche optionnelle 2 : Tâche 5.6.2 – Analyse de la vulnérabilité de la cybersécurité (à l'exclusion des tests de pénétration) et conseils stratégiques au fur et à mesure des besoins.	_____ \$ par jour-personne (TPS/TVH en sus)
Tâche optionnelle 3 : Tâche 5.6.3 – Essais de pénétration, analyse des vulnérabilités et identification des exploits des systèmes et de l'équipement, fournis au besoin.	_____ \$ par jour-personne (TPS/TVH en sus)
Tarif journalier moyen pour les tâches optionnelles 1, 2 et 3 (5.6.1 + 5.6.2 + 5.6.3) / 3	_____ \$ par jour-personne (TPS/TVH en sus)

Afin de calculer la note pour le prix, chaque soumission recevable sera évaluée proportionnellement par rapport au prix évalué le plus bas pour chaque phase conformément au tableau ci-dessous et selon le ratio de 30 %.

Tâches	Tarif journalier total de la soumission	Prix évalué total	Pondération	Nombre maximum de points
5.1 à 5.5	S. O.	Prix total fixe évalué dans la table A de la proposition de coût	50 %	10
5.6 [(5.6.1 + 5.6.2 + 5.6.3) / 3]	Tarif journalier moyen dans la table B de la Proposition de coût	S. O.	50 %	4
Total			100 %	20

Frais de déplacement sur production de reçus

Des déplacements seront nécessaires pour assister à des réunions, animer des séances de consultation, offrir de la formation, effectuer des essais et offrir du soutien technique. Comme indiqué aux points 5 et 6, ils doivent être inclus dans le prix du contrat et seront payés conformément aux dispositions applicables énoncées dans la base de paiement.

L'entrepreneur sera remboursé pour les frais de déplacement autorisés réellement et raisonnablement engagés dans l'exécution des travaux, au prix coûtant, sans aucune indemnité pour les frais généraux ou les bénéfices, conformément aux indemnités relatives aux repas, à l'hébergement et à l'utilisation d'un véhicule privé qui sont précisées aux appendices B, C et D de la *Directive sur les voyages* du Conseil national mixte et selon les autres dispositions de la *Directive*

qui se rapportent aux « voyageurs » plutôt que celles qui se rapportent aux « employés ». Le Canada ne versera à l'entrepreneur aucune indemnité de faux frais pour les voyages autorisés. Tout voyage doit être autorisé au préalable par TC au moyen d'une autorisation de voyage.

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Le coût du temps de déplacement du personnel d'entrepreneur doit être pris en compte dans le prix concurrentiel des tâches 5.1 à 5.5. Le temps de déplacement supplémentaire du personnel pour les travaux relevant des options de la tâche 5.6 sera pris en compte dans le budget défini en fonction des besoins.

Prix maximum total estimé des déplacements 25 000 \$ (TPS/TVH en sus)

Frais de consultation et de formation sur production de reçus

L'entrepreneur sera remboursé pour le lieu, le service de réunion virtuel, l'accueil et le matériel de consultation ou de formation raisonnables nécessaires pour assurer la tenue des séances, au prix coûtant, sans aucune indemnité supplémentaire pour les frais généraux ou la marge bénéficiaire.

Toutes les dépenses d'accueil et d'événements doivent être conformes à la Directive sur les dépenses de voyages, d'accueil, de conférences et d'événements du gouvernement du Canada et autorisées à l'avance par l'autorité technique.

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Pour la préparation des soumissions, le soumissionnaire doit inclure une estimation des frais concernant le lieu, le service de réunion virtuel, l'accueil et le matériel de consultation, comme suit :

Prix total maximum estimé pour la tâche 5.5.1 10 000 \$ (TPS/TVH en sus)

Prix maximum total estimé pour la tâche 5.5.4 90 000 \$ (TPS/TVH en sus)

Frais liés à l'achat d'équipement à mettre à l'essai sur production de reçus

À l'achat d'équipement pour les essais conformément à la tâche 5.6.3, l'entrepreneur sera remboursé au prix coûtant et raisonnable engagé pour l'achat de l'équipement autorisé, sans aucune indemnité supplémentaire pour les frais généraux ou la marge bénéficiaire. Tout achat d'équipement doit être autorisé par le responsable technique par écrit au préalable.

Tout paiement peut faire l'objet d'une vérification par le gouvernement.

Tous les appareils payés dans le cadre de cette tâche par le gouvernement du Canada demeurent la propriété du gouvernement du Canada. À la fin des tests ou à un moment précisé par le responsable technique, les dispositifs sont expédiés, aux frais du gouvernement, à un endroit déterminé par le responsable technique. L'entrepreneur doit utiliser l'emballage d'origine de l'appareil dans la mesure du possible et l'emballer de manière à éviter tout dommage pendant le transport.

Prix total maximum estimé pour la tâche 5.6.3 50 000 \$ (TPS/TVH en sus)

Prix total de la soumission

Remarque : Voir la section « Méthode de sélection » pour connaître la pondération de l'évaluation du prix de la soumission.

<u>Prix de la soumission pour les tâches 5.1 à 5.5 du point 2.1 (tableau A, TPS/TVH en sus)</u>	_____ \$
<u>Prix journalier moyen de la soumission pour la tâche optionnelle 5.6 (tableau B, TPS/TVH en sus)</u>	_____ \$
<u>Prix de la soumission pour les frais de déplacement estimés au point 2.3 (TPS/TVH en sus)</u>	25 000 \$ (TPS/TVH en sus)
<u>Prix de la soumission pour les coûts estimés de consultation/formation au point 2.4 (TPS/TVH en sus)</u>	100 000 \$ (TPS/TVH en sus)
<u>Prix de la soumission pour les coûts d'équipement estimés au point 2.5 (TPS/TVH en sus)</u>	50 000 \$ (TPS/TVH en sus)
<u>Prix total de la soumission (TPS/TVH et tarifs journaliers en sus)</u>	_____ \$

ANNEXE « F » de la PARTIE 3 de la DEMANDE DE SOUMISSIONS

INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

Le soumissionnaire accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

- Carte d'achat VISA ;
- Carte d'achat MasterCard ;
- Dépôt direct (national et international) ;
- Échange de données informatisées (EDI) ;

ANNEXE « G » de la PARTIE 5 de la DEMANDE DE SOUMISSIONS

PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION

Je, soumissionnaire, en présentant les renseignements suivants à l'autorité contractante, atteste que les renseignements fournis sont exacts à la date indiquée ci-dessous. Les attestations fournies au Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un entrepreneur en situation de manquement, si une attestation est jugée fautive, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations d'un soumissionnaire. À défaut de répondre à toute demande ou exigence imposée par le Canada, la soumission peut être déclarée non recevable ou constituer un manquement aux termes du contrat.

Pour obtenir de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, visitez le site Web [d'Emploi et Développement social Canada \(EDSC\) – Travail](#).

Date : _____ (AAAA/MM/JJ) [si aucune date n'est indiquée, la date de clôture de la demande de soumissions sera utilisée]

Compléter à la fois A et B.

A. Cochez seulement une des déclarations suivantes :

- A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.
- A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.
- A3. Le soumissionnaire atteste qu'il est un [employeur sous réglementation fédérale](#), dans le cadre de la [Loi sur l'équité en matière d'emploi](#).
- A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés permanents à temps plein et/ou permanents à temps partiel au Canada.

A5. Le soumissionnaire a un effectif combiné de 100 employés ou plus au Canada; et

- A5.1. Le soumissionnaire atteste qu'il a conclu un [Accord pour la mise en œuvre de l'équité en matière d'emploi](#) valide et en vigueur avec EDSC – Travail.

OU

- A5.2. Le soumissionnaire a présenté l'[Accord pour la mise en œuvre de l'équité en matière d'emploi \(LAB1168\)](#) à EDSC - Travail. Comme il s'agit d'une condition à l'attribution d'un contrat, remplissez le formulaire intitulé Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le à EDSC – Travail.

B. Cochez seulement une des déclarations suivantes :

- B1. Le soumissionnaire n'est pas une coentreprise.

OU

N° de l'invitation - Solicitation No.

T8080-200405

N° de réf. du client - Client Ref. No.

N° de la modif - Amd. No.

File No. - N° du dossier

Id de l'acheteur - Buyer ID

Kristen Scott

N° CCC / CCC No./ N° VME - FMS

() B2. Le soumissionnaire est une coentreprise et chaque membre de la coentreprise doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation. (Consultez la section sur les coentreprises des instructions uniformisées.)

ANNEXE «H»

FORMULAIRE AUTORISATION DE TACHES

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

<p>To Contractor - À L'Entrepreneur: Vendor name here xxxxxxxxxxxxx BPN: 123861098PG0001 Services for / pour:</p>	<p>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.</p>
---	--

Contract Item - No. d' article du contrat	Services (Resources)	Category	\$Rate \$Taux		\$Amount \$Montant
			\$		
			\$		
				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	