RETURN BID TO/ RETOURNER LES SOUMISSIONS À :

receptionsoumission-bidsreceiving.spp@international.gc.ca

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

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

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

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

Comments — Commentaires:

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

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

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

TABLE DES MATIÈRES

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, et toute autre annexe.

1.2 Sommaire

Le Centre de surveillance et d'intervention d'urgence (CISU) s'occupe des communications d'Affaires mondiales Canada (AMC). Ouvert 24 heures par jour et 365 jours par année, il fournit des services consulaires aux Canadiens et aux Canadiennes ayant besoin d'une assistance courante ou d'urgence à l'extérieur du Canada.

AMC exige d'un fournisseur qu'il offre un accès à hauteur de trente (30) utilisateurs à une plateforme Web de logiciels de communication en tant que services (SaaS) qui intègre les applications de clavardage et de conversation mondiales les plus populaires. La plateforme doit au moins comporter les canaux de communication suivants : messagerie instantanée (SMS), application WhatsApp et clavardage en direct (intégrations au site Web).

La plateforme en ligne doit permettre de déployer des outils d'intelligence artificielle ou d'apprentissage machine, comme les des robots conversationnels, qui s'intègrent à tous les canaux de communication. Les robots conversationnels, ainsi que toute interface client sous le contrôle du fournisseur, doivent être disponibles en anglais et en français.

La période du contrat s'échelonne de la date d'attribution du contrat jusqu'à un (1) an plus tard, plus quatre (4) options irrévocables d'une année chacune qui permettent au Canada de prolonger la durée du contrat.

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 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) 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, (2022-03-29) Instructions uniformisées – biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Supprimer : 60 jours
Insérer : 90 jours

2.2 Présentation des soumissions

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de GAC au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

Réception des soumissions d'AMC dans la région de la capitale nationale, l'adresse de courriel est la suivante :

receptionsoumission-bidsreceiving.spp@international.gc.ca

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 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 d'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 5 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 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

La soumission doit être présentée en sections distinctes comme suit :

Section I : Soumission technique
Section II : Soumission financière
Section III : Attestations

En raison du caractère de la demande de soumissions, les soumissions transmises par le service Connexion postel ou par télécopieur ne seront pas acceptées.

Section I : Soumission technique (1 copie par voie électronique par e-mail)

Section II : Soumission financière (1 copie par voie électronique par e-mail)

Section III : Attestations (1 copie par voie électronique par e-mail)

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

Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-dessous pour préparer leur soumission en version papier.

a) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm);
b) utiliser un système de numérotation correspondant à celui de la demande de soumissions.

En avril 2006, le Canada a adopté une politique exigeant que les ministères et organismes fédéraux prennent les mesures nécessaires pour tenir compte des facteurs environnementaux dans le processus d'approvisionnement : la Politique d'achats écologiques (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32573). Pour aider le Canada à atteindre ses objectifs, les soumissionnaires devraient :

1. Inclure toutes les certifications environnementales pertinentes pour votre organisation (p. ex., ISO 14001, Leadership in Energy and Environmental Design (LEED), Carbon Disclosure Project, etc.)
2. Inclure toutes les certifications environnementales ou déclarations environnementales de produit (DEP) propres à votre produit ou service (p. ex., Forest Stewardship Council [FSC], ENERGYSTAR, etc.)
3. Sauf indication contraire, les soumissionnaires sont encouragés à présenter leurs soumissions par voie électronique. Si des versions papier sont requises, les soumissionnaires devraient :
    a. utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et contenant au moins 30 % de matières recyclées; et
    b. utiliser un format qui respecte l'environnement : impression noir et blanc plutôt qu'en couleur, recto verso/à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ou reliure à anneaux.

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

3.1.1 Les soumissionnaires doivent présenter leur soumission financière en conformité avec la base de paiement reproduite à l'annexe B

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 E Instruments de paiement électronique, afin d'identifier lesquels sont acceptés.

Si l'annexe E 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.

3.1.3 Fluctuation du taux de change

C3010T (2013-11-06), Fluctuation du taux de change – Atténuation des risques,

Le besoin ne prévoit pas offrir d'atténuer les risques liés à la fluctuation du taux de change. Aucune demande d'atténuation des risques liés à la fluctuation du taux de change ne sera prise en considération. Toute soumission incluant une telle disposition sera déclarée non recevable.

3.1.4 Clauses du *Guide des CCUA*

Section III : Attestations
Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5.

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.

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 Attachement 4.1.

4.1.2 Criteres financiers

4.1.2.1 Critères financiers obligatoires

Clause du *Guide des CCUA* A0222T (2-14-06-26), Évaluation du prix-soumissionnaires établis au Canada et à l'étranger

1. Le prix de la soumission sera évalué comme suit :

   a. les soumissionnaires établis au Canada doivent proposer des prix fermes, les droits de douane et les taxes d'accise canadiens compris, et les taxes applicables exclues.

   b. les soumissionnaires établis à l'étranger doivent proposer des prix fermes, les droits de douane, les taxes d'accise canadiens et les taxes applicables exclus. Les droits de douane et les taxes d'accise canadiens payables par le Canada seront ajoutés, pour les besoins de l'évaluation seulement, aux prix présentés par les soumissionnaires établis à l'étranger.

2. Sauf lorsque la demande de soumissions précise que les soumissions doivent être présentées en dollars canadiens, les soumissions présentées en devises étrangères seront converties en dollars canadiens pour les besoins de l'évaluation. Pour les soumissions présentées en devises étrangères, le taux indiqué par la Banque du Canada à la date de clôture des soumissions, ou à une autre date précisée dans la demande de soumissions, sera utilisé comme facteur de conversion.

3. Bien que le Canada se réserve le droit d'attribuer le contrat FAB usine ou FAB destination, le Canada demande que les soumissionnaires proposent des prix FAB usine ou point d'expédition et FAB destination. Les soumissions seront évaluées sur une base FAB destination.

4. Pour les fins de la demande de soumissions, les soumissionnaires qui ont une adresse au Canada sont considérés comme étant des soumissionnaires établis au Canada, et les soumissionnaires qui ont une adresse à l'extérieur du Canada sont considérés comme étant des soumissionnaires établis à l'étranger.

4.2 Méthode de sélection

1. Pour être déclarée recevable, une soumission doit :
    a. respecter toutes les exigences de la demande de soumissions; et
    b. satisfaire à tous les critères obligatoires; et
    c. obtenir le nombre minimal de points requis pour l'évaluation technique ; et
2. Les soumissions qui ne répondent pas aux exigences a) ou b) ou c) seront déclarées non recevables.
3. La sélection sera faite en fonction du meilleur résultat global sur le plan du mérite technique et du prix. Une proportion de 70% sera accordée au mérite technique et une proportion de 30% sera accordée au prix.
4. Afin de déterminer la note pour le mérite technique, la note technique globale de chaque soumission recevable sera calculée comme suit : le nombre total de points obtenus sera divisé par le nombre total de points pouvant être accordés, puis multiplié par 70%.
5. Afin de déterminer la note pour le prix, chaque soumission recevable sera évaluée proportionnellement au prix évalué le plus bas et selon le ratio de 30%.
6. Pour chaque soumission recevable, la cotation du mérite technique et la cotation du prix seront ajoutées pour déterminer la note combinée.
7. La soumission recevable ayant obtenu le plus de points ou celle ayant le prix évalué le plus bas ne sera pas nécessairement choisie. La soumission recevable qui obtiendra la note combinée la plus élevée pour le mérite technique et le prix sera recommandée pour l'attribution du contrat.

[Le tableau ci-dessous présente un exemple où les trois soumissions sont recevables et où la sélection de l'entrepreneur se fait en fonction d'un ratio de 70/30 à l'égard du mérite technique et du prix, respectivement.] Le nombre total de points pouvant être accordé est de 135, et le prix évalué le plus bas est de 45 000,00 $ (45).

Base de sélection - l'égard du mérite technique **(70%)** et du prix (**30%)**			
Soummissionaire	**Soummissionaire 1**	**Soummissionaire 2**	**Soummissionaire 3**
Note technique globale	OS1: 120/135	OS2: 98/135	OS3: 82/135
Prix évalué de la soumission	P1: C$60,000.00	P2: C$55,000.00	LP and P3: $50,000.00
Calculs	**Note pour le mérite technique (OS1 X70)**	**Note pour le prix (LP/P1 X 30)**	**Note combinée**
Bidder 1	120/135 x 70 = 62.22	50/60 x 30 = 24.99	87.21
Bidder 2	98/135 x 70 = 50.81	50/55 x 30 = 27.27	78.08
Bidder 3	82/135 x 70 = 42.51	50/50 x 30 = 30.00	72.51

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 fausse, 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), 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), 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.

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.

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;

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.

   2. 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 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 et à la soumission technique de l'entrepreneur intitulée _____, en date du _____.

7.1.1 Biens et(ou) services facultatifs

L'autorité contractante peut exercer l'option à n'importe quel moment avant la date d'expiration du contrat en envoyant un avis écrit à 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) publié par Travaux publics et Services gouvernementaux Canada.

7.2.1 Conditions générales

2035 (2022-05-12), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

7.2.2 Conditions générales supplémentaires

N0004C (2020-05-08), s'appliquent au contrat et en font partie intégrante.

- **Responsabilité de la première partie**

  Exécution du contrat: L'entrepreneur est entièrement responsable envers le Canada de tous les dommages résultant de l'exécution ou l'inexécution du contrat par l'entrepreneur.

  Violation des données: L'entrepreneur est entièrement responsable envers le Canada de tous les dommages qui résultent d'un manquement qu'il a commis aux obligations en matière de sécurité ou de confidentialité et qui entraîne un accès non autorisé à des documents, des données ou de l'information appartenant au Canada ou à un tiers, ou leur divulgation non autorisée.

  Limitation par incident: Sous réserve de l'article suivant, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale de l'entrepreneur par incident n'excédera pas la valeur cumulative des factures contractuelles pour les 12 mois précédant l'incident.
  Aucune limite : La limite fixée ci-dessus pour la responsabilité de l'entrepreneur ne s'applique pas aux éléments suivants :

  a. inconduite volontaire ou actes délibérément fautifs; et

  b. tout manquement aux obligations en matière de garantie.

  Responsabilité envers les tiers: Que la réclamation d'un tiers soit faite au Canada, à l'entrepreneur ou aux deux, chaque partie convient qu'elle acceptera l'entière responsabilité des dommages qu'elle cause au tiers dans le cadre du contrat. La répartition de la

responsabilité correspondra au montant convenu par les parties ou déterminé par la cour. Les parties conviennent de se rembourser pour tout paiement à un tiers relativement aux dommages causés par l'autre. L'autre partie accepte d'effectuer promptement le remboursement pour sa part de responsabilité.

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.

7.3.2 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.

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 1 an plus tard inclusivement.

7.4.3 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus _4_ période(s) supplémentaire(s) de _1_ année(s) chacune, selon les mêmes conditions. L'entrepreneur accepte que pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de paiement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur au moins 30 jours civils avant la date d'expiration du 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

7.5 Responsables

7.5.1 Autorité contractante

L'autorité contractante pour le contrat est:

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

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 : (à insérer à 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 insérer à l'attribution du contrat)

7.6 Divulgation 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

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé un prix ferme l'annexe B. Les droits de douane et les taxes applicables sont en sus.

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 Limitation des dépenses

1. La responsabilité totale du Canada envers l'entrepreneur en vertu du contrat ne doit pas dépasser la somme de 600,000.00$. Les droits de et les taxes applicables sont en sus.

2. Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux découlant de tout changement de conception, de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements de conception, modifications ou interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés

aux travaux. L'entrepreneur n'est pas tenu d'exécuter des travaux ou de fournir des services qui entraîneraient une augmentation de la responsabilité totale du Canada à moins que l'augmentation n'ait été autorisée par écrit par l'autorité contractante. L'entrepreneur doit informer, par écrit, l'autorité contractante concernant la suffisance de cette somme :

a. lorsque 75 % de la somme est engagée, ou

b. quatre mois avant la date d'expiration du contrat, ou

c. dès que l'entrepreneur juge que les fonds du contrat sont insuffisants pour l'achèvement des travaux,

selon la première de ces conditions à se présenter.

3. Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds additionnels requis. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada à son égard.

7.7.3 Paiement unique

Le Canada paiera l'entrepreneur lorsque les travaux seront complétés et livrés conformément aux dispositions de paiement du contrat si :

a. une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis conformément aux instructions de facturation prévues au contrat;

b. tous ces documents ont été vérifiés par le Canada;

c. les travaux livrés ont été acceptés par le Canada.

7.7.4 Paiement électronique de factures – contrat

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

a. Dépôt direct (national et international) ;

7.8 Instructions relatives à la facturation

1. L'entrepreneur doit soumettre ses factures conformément à l'article intitulé « Présentation des factures » des conditions générales. Les factures ne doivent pas être soumises avant que tous les travaux identifiés sur la facture soient complétés.

2. Un (1) exemplaire doit être envoyé à l'autorité contractante identifiée sous l'article intitulé « Responsables » du contrat.

7.9 Attestations et renseignements supplémentaires

7.9.1 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.

7.10 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.

7.11 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 N0004C (2020-05-08), Limitation de la responsabilitéc)
c) les conditions générales – 2035 (2022-05-12) 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 ;
g) l'Annexe D, Liste de vérification des exigences relatives à la sécurité de l'informatique ;
h) l 'Annexe E, Electronic Payment Instrument
I) Annex F, Federal Contractors Program for Employment Equity – Certification
j) Attachement 4.1, Evaluation des critères de soumission ;
k) la soumission de l'entrepreneur datée du _____, (*inscrire la date de la soumission*) (*si la soumission a été clarifiée ou modifiée, insérer au moment de l'attribution du contrat :* « clarifiée le _____ » ***ou*** « modifiée le _____ » *et inscrire la ou les dates des clarifications ou modifications*) y compris son PAI (*s'il y a lieu)*.

7.12 Ressortissants étrangers (entrepreneur canadien OU entrepreneur étranger)

Clause du *Guide des CCUA* A2000C (2006-06-15), Ressortissants étrangers (entrepreneur canadien)

Où

Clause du *Guide des CCUA* A2001C (2006-06-16), Ressortissants étrangers (entrepreneur étranger)

7.13 Assurances ou Exigences en matière d'assurance

Clause du *Guide des CCUA* G1005C (2016-01-28), Assurance – aucune exigence particulière

7.14 Limitation de la responsabilité - Logiciels-services (SaaS) dans un nuage public

- **Responsabilité de la première partie**
  - **Exécution du contrat :** L'entrepreneur est entièrement responsable envers le Canada de tous les dommages résultant de l'exécution ou l'inexécution du contrat par l'entrepreneur.

- **Violation des données :** L'entrepreneur est entièrement responsable envers le Canada de tous les dommages qui résultent d'un manquement qu'il a commis aux obligations en matière de sécurité ou de confidentialité et qui entraîne un accès non autorisé à des documents, des données ou de l'information appartenant au Canada ou à un tiers, ou leur divulgation non autorisée.

- **Limitation par incident :** Sous réserve de l'article suivant, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale de l'entrepreneur par incident n'excédera pas la valeur cumulative des factures contractuelles pour les 12 mois précédant l'incident.

- **Aucune limite :** La limite fixée ci-dessus pour la responsabilité de l'entrepreneur ne s'applique pas aux éléments suivants :

  a. inconduite volontaire ou actes délibérément fautifs; et

  b. tout manquement aux obligations en matière de garantie.

- **Responsabilité envers les tiers :** Que la réclamation d'un tiers soit faite au Canada, à l'entrepreneur ou aux deux, chaque partie convient qu'elle acceptera l'entière responsabilité des dommages qu'elle cause au tiers dans le cadre du contrat. La répartition de la responsabilité correspondra au montant convenu par les parties ou déterminé par la cour. Les parties conviennent de se rembourser pour tout paiement à un tiers relativement aux dommages causés par l'autre. L'autre partie accepte d'effectuer promptement le remboursement pour sa part de responsabilité.

7.15 Règlement des différends

(a) Les parties conviennent de maintenir une communication ouverte et honnête concernant les travaux pendant toute la durée de l'exécution du marché et après.

(b) Les parties conviennent de se consulter et de collaborer dans l'exécution du marché, d'informer rapidement toute autre partie des problèmes ou des différends qui peuvent survenir et de tenter de les résoudre.

(c) Si les parties n'arrivent pas à résoudre un différend au moyen de la consultation et de la collaboration, les parties conviennent de consulter un tiers neutre offrant des services de règlement extrajudiciaire des différends pour tenter de régler le problème.

(d) Vous trouverez des choix de services de règlement extrajudiciaire des différends sur le site Web Achats et ventes du Canada sous le titre « Règlement des différends ».

ANNEXE « A » ÉNONCÉ DES TRAVAUX

1. Objectif

L'objectif de la présente demande de propositions (DP) consiste à identifier un fournisseur commercial qui fournira au une plateforme de communication à canaux multiples sous la forme d'un SaaS, qui sera utilisée par le CISU d'AMC.

2. Contexte

Le Centre de surveillance et d'intervention d'urgence (CISU) s'occupe des communications d'Affaires mondiales Canada (AMC). Ouvert 24 heures par jour et 365 jours par année, il fournit des services consulaires aux Canadiens et aux Canadiennes ayant besoin d'une assistance courante ou d'urgence à l'extérieur du Canada.

Le CISU peut recevoir plus de 500 demandes à l'heure en situation d'urgence, comme ce fut le cas en raison des activités de rapatriement mondial causées par la pandémie de COVID-19. Pour concrétiser sa stratégie de gestion du flux de travail, le CISU a l'intention de tirer parti de l'intelligence artificielle, de l'apprentissage machine et du traitement du langage naturel pour automatiser les réponses aux demandes de renseignements courantes provenant des applications de conversation ou de clavardage en direct incorporées aux sites Web ministériels.

Avant 2021, tout ressortissant canadien en détresse à l'étranger pouvait communiquer avec le CISU par téléphone, télécopieur, SMS ou courriel. En 2021, un projet pilote a été mis en place pour introduire des canaux de communication supplémentaires, notamment le clavardage en direct et WhatsApp. Le projet pilote a fourni une plateforme Web de type SaaS intégrant ces canaux en un centre de mobilisation unifié. La plateforme du projet pilote pouvait intégrer des médias sociaux et des applications de clavardage supplémentaires et s'appuyait sur des outils avancés de gestion des flux de travail faisant appel à l'intelligence artificielle, à l'apprentissage machine et au traitement du langage naturel.

3. Portée

Le fournisseur doit offrir un accès à hauteur de trente (30) utilisateurs à une plateforme Web de logiciels de communication en tant que services (SaaS) qui intègre les applications de clavardage et de conversation mondiales les plus populaires. La plateforme doit au moins comporter les canaux de communication suivants : messagerie instantanée (SMS), application WhatsApp et clavardage en direct (intégrations au site Web).

La plateforme en ligne doit permettre de déployer des outils d'intelligence artificielle ou d'apprentissage machine, comme les robots conversationnels, qui s'intègrent à tous les canaux de communication. Les robots conversationnels, ainsi que toute interface client sous le contrôle du fournisseur, doivent être disponibles en anglais et en français.

La plateforme doit fournir les outils suivants :

- supervision et soutien de gestion, comme la surveillance des séances de clavardage et l'examen des transcriptions;
- analyse de données et analytique;
- automatisation des flux de travail, comme l'acheminement des messages et la gestion des files d'attente, ainsi que les déclencheurs et les réponses automatiques;
- intégration d'applications de tiers, notamment avec Microsoft Dynamics 365;
- bases de connaissances (idéalement prédictives) qui appuient les réponses des agents au moyen de sources d'information recommandées ou de suggestions de réponses prédéfinies.

4. Exclusions

Les appels vocaux entrants acheminés par le système d'autocommutateurs privés (PBX) d'AMC ne seront pas traités au moyen de la plateforme de communication à canaux multiples. Toutefois, cette dernière doit pouvoir gérer les communications vocales acheminées par une application de clavardage.

Le fournisseur n'est pas tenu d'obtenir ou de créer des comptes d'application de clavardage au nom d'AMC.

5. Spécifications techniques

L'outil doit :

- être offert selon le modèle SaaS;
- incorporer tous les canaux de communication dans un seul centre de mobilisation;
- au moins comporter les canaux de communication suivants : messagerie instantanée (SMS), application WhatsApp et clavardage en direct;
- être en mesure d'intégrer et d'abandonner de nouveaux canaux en réponse à l'évolution des modes d'utilisation des médias sociaux et des applications de clavardage;
- incorporer des outils d'automatisation du flux de travail – messages de réponse normalisés, messages de réponse automatisés, acheminement des messages, etc.;
- avoir la capacité d'exporter des données de conversation;
- prendre en charge en plusieurs langues, dont l'anglais et le français;
- permettre l'intégration d'applications de tiers, notamment avec Microsoft Dynamics 365;
- disposer d'un cadre souple permettant la conservation et l'élimination des données et qui peut être harmonisé avec les exigences d'AMC;
- fonctionner avec un haut niveau de disponibilité et les mécanismes de redondance des centres de données;
- traiter et stocker toutes les données au Canada;
- répondre aux normes de sécurité technique, notamment ISO/IEC 27001:2013 (ou ISO 27001) et ICPA SOC 2, type II;
- fournir un soutien technique ininterrompu (24 heures sur 24, 7 jours sur 7) aux agents des centres de contact et offrir des mécanismes d'acheminement appropriés.

Le fournisseur doit offrir au client trente (30) accès à l'outil en ligne. Ces utilisateurs doivent pouvoir accéder et utiliser l'outil en même temps.

La formation à distance doit porter sur :

- l'accès à l'outil;
- l'utilisation de l'outil par l'agent pour communiquer avec les clients;
- l'utilisation de l'outil par l'administrateur pour gérer les utilisateurs et configurer le système;
- la configuration et l'utilisation d'outils de traitement du langage naturel, d'apprentissage machine et d'intelligence artificielle;
- la configuration et la production de rapports personnalisés et la réalisation d'analyses de données.

6. Déplacements

Aucun déplacement ne sera nécessaire dans le cadre de l'exécution du présent contrat. Toutes les activités de formation et de soutien doivent être réalisées à distance.

7. Contraintes

Le fournisseur doit utiliser ses propres systèmes pour fournir les produits livrables, puisqu'il n'a pas accès directement aux systèmes du client. L'équipement fourni par le gouvernement, les outils, les installations, etc. ne sont pas destinés à la réalisation du présent projet.

8. Soutien aux clients

Le responsable du projet du client doit se mettre à la disposition du fournisseur par courriel ou par téléphone, au besoin, pendant les heures normales de travail (de 9 h à 17 h, heure normale de l'Est) pendant la semaine (du lundi au vendredi) pour la durée du contrat afin de répondre à toute demande de renseignements connexe.

9. Produits livrables

a. Accès pour un maximum de trente (30) utilisateurs et pendant une période de douze (12) mois à une plateforme de communication à canaux multiples SaaS en ligne qui doit être opérationnelle et accessible par le client à partir de la date de début du contrat.

b. Séances de formation portant sur tous les aspects de l'utilisation de l'outil.

c. Soutien technique ininterrompu.

ANNEXE « B » BASE DE PAIEMENT

Quantités estimées aux fins d'évaluation seulement

Les quantités estimées suivantes seront utilisées pour la période du contrat qui s'étend du 1er janvier 2023 au 31 décembre 2023.

Exigence	Unité	Volumes annuels estimés	Prix
Frais d'installation	Une seule fois	1	
Les frais mensuels incluent toutes les exigences précisées dans l'Énoncé des travaux pour un maximum de 30 utilisateurs simultanés, y compris les communications illimitées utilisant tous les canaux de communication.	Par mois	12 mois	
Formation d'un maximum de 30 utilisateurs sur tous les aspects de l'utilisation de la plateforme.	Par heure	10 heures	

Quantités estimées pour la période d'options

1re année optionnelle, du 1er janvier 2024 au 31 décembre 2024

Exigence	Unité	Volumes annuels estimés	Prix
Les frais mensuels incluent toutes les exigences précisées dans l'Énoncé des travaux pour un maximum de 30 utilisateurs simultanés, y compris les communications illimitées utilisant tous les canaux de communication.	Par mois	12 mois	
Formation d'un maximum de 30 utilisateurs sur tous les aspects de l'utilisation de la plateforme.	Par heure	10 heures	

2e année optionnelle, du 1er janvier 2025 au 31 décembre 2025

Exigence	Unité	Volumes annuels estimés	Prix
Les frais mensuels incluent toutes les exigences précisées dans l'Énoncé des travaux pour un maximum de 30 utilisateurs simultanés, y compris les communications illimitées utilisant tous les canaux de communication.	Par mois	12 mois	
Formation d'un maximum de 30 utilisateurs sur tous les aspects de l'utilisation de la plateforme.	Par heure	10 heures	

3e année optionnelle, du 1er septembre 2026 au 31 décembre 2026

Exigence	Unité	Volumes annuels estimés	Prix
Les frais mensuels incluent toutes les exigences précisées dans l'Énoncé des travaux pour un maximum de 30 utilisateurs simultanés, y compris les communications illimitées utilisant tous les canaux de communication.	Par mois	12 mois	
Formation d'un maximum de 30 utilisateurs sur tous les aspects de l'utilisation de la plateforme.	Par heure	10 heures	

4e année optionnelle, du 1er septembre 2027 au 31 décembre 2027

Exigence	Unité	Volumes annuels estimés	Prix
Les frais mensuels incluent toutes les exigences précisées dans l'Énoncé des travaux pour un maximum de 30 utilisateurs simultanés, y compris les communications illimitées utilisant tous les canaux de communication.	Par mois	12 mois	
Formation d'un maximum de 30 utilisateurs sur tous les aspects de l'utilisation de la plateforme.	Par heure	10 heures	

ANNEXE « C » LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Government of Canada / Gouvernement du Canada

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

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Global Affairs Canada	CSW/CSD/CFM

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work - Brève description du travail

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

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

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

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

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

Canada ☐	NATO / OTAN ☐	Foreign / Étranger ☐

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

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

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

Canada	NATO / OTAN	Foreign / Étranger
PROTECTED A / PROTÉGÉ A ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Security Classification / Classification de sécurité

TBS/SCT 350-103 (2004/12)

Canada

Government of Canada / Gouvernement du Canada

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

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

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

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

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

Special comments: Unclass
Commentaires spéciaux :

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

10. b) May unscreened personnel be used for portions of the work? — ☐ No / Non ☑ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted: — ☐ No / Non ☑ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

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

PART C *(continued)* / PARTIE C *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

ANNEXE « D » Annexe technique sur les exigences en matière de sécurité de la TI
(pour le traitement, la production et le stockage dans le nuage d'information sensible jusqu'au niveau « Protégé A »)
Affaires mondiales Canada (AMC)

Justification

La présente annexe technique sur la sécurité de la TI a été conçue spécialement pour les demandes de propositions (DP) qui nécessiteront de traiter, de produire ou de stocker de l'information d'AMC dans le nuage par l'entremise d'une solution d'un fournisseur de services infonuagiques (FSI).

Cette annexe sur la sécurité de la TI vise l'information cotée jusqu'au niveau **« Protégé A »**.

1.0 Avant-propos

En plus de la Liste de vérification relative à la sécurité (LVERS), la présente annexe décrit les exigences en matière de sécurité pour la protection d'information de niveau **« Protégé A »** produite, traitée ou stockée en vertu de ce contrat, y compris :

a) les systèmes de gestion/technologie de l'information (GI/TI) de l'entrepreneur servant à traiter, à produire ou à stocker l'information **« Protégé A »**;
b) les systèmes de gestion/technologie de l'information (GI/TI) du courtier d'infonuagique/de services infonuagiques (CSI) servant à traiter, à produire ou à stocker l'information **« Protégé A »**;
c) les couches d'infrastructure sous forme de service (IaaS), de plateforme sous forme de service (PaaS) ou de logiciels sous forme de service (SaaS) d'un tiers fournisseur de services/solutions infonuagiques (FSI) utilisées dans la prestation de services en vertu du présent contrat.

La divulgation sans autorisation d'information de niveau **« Protégé A »** risque de porter préjudice à une personne, à une organisation ou à un gouvernement. AMC et l'entrepreneur conviennent donc de maximiser la sécurité de la solution, conformément aux exigences stipulées dans la présente annexe technique en matière de sécurité.

2.0 Attestations

2.1 L'entrepreneur doit démontrer, avant l'attribution du contrat, que le FSI a reçu **au moins une** des certifications suivantes attribuées par des tierces parties de l'industrie[1] :

- Conformité à la norme 27001 de l'Organisation internationale de normalisation (ISO);

OU

- Conformité à la norme Service Organization Controls (SOC) de type II de l'American Institute of Certified Public Accountants (AICPA).

[1] FedRAMP, "Attestation Security, Trust and Assurance Registry (STAR) de niveau 2 de la Cloud Security Alliance (CSA)", Conformité à la norme de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS), et autres certifications pourraient être considérées durant l'évaluation mais ne remplaceront pas les certifications attribuées par des tierces parties mentionnées ici.

2.2 L'entrepreneur doit démontrer, avant l'attribution du contrat, que le FSI a réalisé une autoévaluation selon la Cloud Controls Matrix de la CSA, aussi connue sous le nom de Security, Trust and Assurance Registry (STAR) de niveau 1. Une attestation Security, Trust and Assurance Registry (STAR) de niveau 2 de la CSA peut être acceptée comme substitut.

2.3 L'entrepreneur doit s'assurer que les certifications présentées pour démontrer la conformité du fournisseur de services infonuagiques aux exigences relatives à la sécurité sont maintenues et valides pour toute la durée du contrat. L'entrepreneur doit également préciser si l'attestation ou la norme d'audit s'applique à l'ensemble ou à une partie de la solution.

2.4 L'entrepreneur doit fournir une preuve de sa ou ses certifications en matière de sécurité et toutes les normes de vérification applicables pour sa solution proposée, sous forme de certificat ou de norme de vérification valide, et décrire comment la certification ou la norme de vérification a été évaluée et obtenue (c.-à-d. rapports de vérification ou certifications d'un tiers de l'industrie) pour chaque certification et norme de vérification détenue. Une certification par une tierce partie doit être délivrée par une tierce partie indépendante qui est tenue d'être objective et d'appliquer des normes professionnelles aux preuves qu'elle examine et produit.

3.0 Exigences en matière de sécurité et traçabilité

Les ministères ont besoin de mesures de protection progressives qui correspondent aux risques visant leurs renseignements et leurs biens de TI. Des profils de sécurité sont établis pour appuyer cette exigence.

Un profil de sécurité de base est un ensemble de contrôles de sécurité de la TI qu'établit une organisation comme exigences obligatoires minimales pour ses systèmes informatiques. En respectant un ensemble normalisé de contrôles de sécurité, les ministères peuvent :

- cerner et évaluer les risques;
- élaborer des stratégies pour atténuer les risques de façon appropriée.

Le guide sur la sécurité de la TI 33 (ITSG-33) du Centre de la sécurité des télécommunications (CST)[2] contient des définitions de contrôles de la sécurité qu'utilise AMC comme base pour la protection des systèmes informatiques du gouvernement du Canada et la gestion des risques pour la sécurité visant la TI. Une connaissance du glossaire de l'ITSG-33[3] et, plus particulièrement, des contrôles décrits à l'*Annexe 3A – Catalogue des contrôles de sécurité (ITSG-33)*[4] sera bénéfique dans le dialogue avec les praticiens de la sécurité d'AMC qui participeront à l'élaboration et à l'évaluation de la solution.

Le profil de sécurité de base du gouvernement du Canada pour ses services infonuagiques de TI définit les contrôles de sécurité de base recommandés pour la mise en œuvre par des FSI et les ministères fédéraux afin de protéger adéquatement les services infonuagiques ayant une catégorie de sécurité **« Protégé A »**.

3.1 L'entrepreneur doit collaborer avec les praticiens de la sécurité d'AMC afin de cerner, de comprendre et de consigner les risques visant l'application. Cet effort sert à cerner les risques

[2] https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie
[3] https://cyber.gc.ca/fr/orientation/annexe-5-glossaire-itsg-33
[4] https://cyber.gc.ca/fr/orientation/annexe-3a-catalogue-des-controles-de-securite-itsg-33

clés pour les biens et les fonctions d'importance que fournit l'application, ainsi qu'à établir une base en vue de la sélection et de l'adaptation de l'ensemble de contrôles de sécurité de base défini dans le **Profil des mesures de sécurité pour les services de TI du gouvernement du Canada fondés sur l'informatique en nuage d'Affaires mondiales Canada** fourni par le Secrétariat du Conseil du Trésor (SCT) (guide du SCT sur la MTES concernant les applications SaaS jusqu'au niveau « Protégé B »). Fournir le document n° **14310732** accessible sur Infobanque aux soumissionnaires, sur demande.

3.2 L'entrepreneur doit respecter toutes les exigences de sécurité identifiées par un « *Yes* » dans la colonne « *TBS Playbook PBMM Controls* » du **Profil des mesures de sécurité pour les services de TI du gouvernement du Canada fondés sur l'informatique en nuage d'Affaires mondiales Canada**. Certains contrôles pourraient être exclus dans le cadre du processus d'adaptation. L'exclusion de contrôles de sécurité dépendra des menaces et des risques cernés avec la solution proposée et la classification des données.

3.3 L'entrepreneur doit collaborer avec les praticiens de la sécurité d'AMC dans l'adaptation des exigences détaillées en matière de sécurité afin d'atteindre un risque acceptable dans la définition de la solution. On peut satisfaire aux exigences en matière de sécurité grâce à des certifications de l'industrie (voir la section 2.0, *Certifications*), à des logiciels personnalisés, à des logiciels de tiers, à une plateforme et/ou à des éléments d'infrastructure. La version adaptée du **Profil des mesures de sécurité pour les services de TI du gouvernement du Canada fondés sur l'informatique en nuage d'Affaires mondiales Canada** sera connue sous le nom de **Matrice de traçabilité des exigences relatives à la sécurité (MTES)**.

3.4 L'entrepreneur doit cerner et tracer les contrôles de sécurité satisfaits à l'aide de n'importe quelle certification (voir la section 2.0, *Certifications*) dans la MTES. L'entrepreneur doit consigner tous les autres contrôles de sécurité et assurer que ces derniers sont compris dans la portée du processus d'adaptation, conformément au processus d'évaluation et d'autorisation de sécurité (EAS) (voir la section 15.0, *Évaluation et autorisation de sécurité [EAS]*).

3.5 Conformément au processus d'EAS (voir la section 15.0, *Évaluation et autorisation de sécurité [EAS]*), l'entrepreneur doit fournir de la documentation expliquant clairement la conception qui répondra à chacune des exigences en matière de sécurité. Dans la plupart des cas, cette documentation décrit les mécanismes de sécurité, l'endroit où les mécanismes s'inscrivent dans l'architecture et tous les modèles de conception pertinents pour en assurer l'utilisation correcte. La conception doit spécifier clairement si le soutien est assuré par un logiciel personnalisé, un logiciel d'un tiers, la plateforme ou l'infrastructure.

4.0 Exigences relatives au personnel

4.1 Rôle de l'architecte de la sécurité

4.1.1 L'entrepreneur doit confier la responsabilité de la sécurité à une seule ressource technique supérieure, soit l'architecte de la sécurité. Cet architecte doit certifier la sécurité de chaque produit à livrer. La certification sera désignée comme le « Dossier de certification de sécurité ».

4.2 Exigences relatives au personnel de soutien opérationnel

4.2.1 Citoyenneté et résidence

4.2.1.1 Tous les membres du personnel opérationnel de l'entrepreneur affectés au bureau de service, au centre des opérations de sécurité (COS) et au centre d'exploitation de réseau (CER) pour l'ensemble de la solution du fournisseur doivent être des citoyens du Canada et/ou de pays avec lesquels le Canada a négocié des ententes internationales bilatérales en matière de sécurité (EIBMS)[5], ou de pays membres de l'Union européenne (UE) ou de l'OTAN.

4.2.1.2 Tous les membres du personnel opérationnel de l'entrepreneur affectés au bureau de service, au COS et au CER pour l'ensemble de la solution du fournisseur doivent habiter au Canada ou dans des pays avec lesquels le Canada a négocié des EIBMS, ou dans des pays membres de l'UE ou de l'OTAN.

4.2.2 Vérification des antécédents

4.2.2.1 L'entrepreneur doit fournir une preuve de la fiabilité de tous les membres du personnel opérationnel qui accomplissent des fonctions administratives pour la solution proposée, et ce, grâce à un processus documenté de contrôle de la sécurité. L'enquête de sécurité doit exiger soit :

a) une preuve de « cote de fiabilité » délivrée par Services publics et Approvisionnement Canada (SPAC);
b) une autoévaluation pour un processus équivalent à celui de l'entrepreneur qui comprend une vérification des antécédents des cinq dernières années, notamment :
    (i) une vérification de l'identité exigeant au moins deux instances de preuves d'identité, dont une doit être une preuve d'identité essentielle (c.-à-d. un document d'identité fourni par un gouvernement, comme un certificat de naissance, un passeport ou un permis de conduire);
    (ii) une vérification du casier judiciaire;
    (iii) une vérification du crédit.

4.2.2.2 Tout candidat ou membre actuel du personnel opérationnel qui a été accusé devant un tribunal **est inacceptable** jusqu'à ce que les accusations criminelles aient été résolues. Sur demande, l'entrepreneur doit fournir de la documentation attestant d'une adjudication favorable des vérifications des antécédents pour tout le personnel appuyant le système.

5.0 Centres des opérations

5.1 Le centre des opérations de la sécurité (COS), le centre d'exploitation de réseau (CER) et le bureau de service devraient être situés physiquement et exploités au Canada, dans des pays avec lesquels le Canada a conclu des EIBMS ou dans des pays membres de l'UE ou de l'OTAN.

6.0 Conformité avec l'Avis de mise en œuvre de la Politique sur la sécurité (AMOPS)

6.1 Orientation du SCT sur l'utilisation sécurisée des services commerciaux d'informatique en nuage (AMOPS 2017-01)

[5] https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html, section *Instruments de sécurité internationaux*.

6.1.1 Conformément à l'Orientation du SCT sur l'utilisation sécurisée des services commerciaux d'informatique en nuage[6], l'entrepreneur doit s'assurer que :

a) la solution permet l'identification et l'authentification des personnes et des appareils avec un niveau d'assurance approprié avant que ces personnes ou appareils puissent avoir accès aux renseignements et aux services hébergés dans les services infonuagiques. Une telle authentification doit respecter la Norme sur l'assurance de l'identité et des justificatifs[7] et est conforme aux services d'identité et d'authentification d'entreprise du gouvernement du Canada;
b) l'accès est limité au personnel selon les principes du droit d'accès minimal, du besoin de savoir et de la séparation des tâches, et il est appuyé par des contrôles de sécurité appropriés. La restriction de l'accès comprend :
    (i) l'établissement de restrictions de l'usage et de configurations des appareils appropriées;
    (ii) la prise en considération du contexte de menace lorsqu'on accède aux services infonuagiques;
c) l'accès privilégié des utilisateurs aux services infonuagiques met en œuvre et configure des mécanismes d'authentification plus solides (authentification à facteurs multiples), qui respectent le document ITSP.30.031 V3 du CST, *Conseils en matière de sécurité des technologies de l'information pour les praticiens*[8]. Des mesures de sécurité supplémentaires, comme l'utilisation de postes de travail à accès privilégié et de réseaux de gestion dédiés, pourraient également être nécessaires pour atténuer davantage les risques associés à l'accès privilégié.
d) les réseaux de transit de données sont protégés adéquatement grâce à l'utilisation de dispositifs de chiffrement et de mesures de protection des réseaux appropriées. Les services fondés sur l'informatique en nuage doivent utiliser les algorithmes cryptographiques et des protocoles réseau approuvés par le CST, comme il est précisé dans les documents suivants :
    - ITSP.40.111, Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B du CST;
    - ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* du CST;
e) des processus et procédures robustes de gestion des clés sont mis en œuvre afin de protéger les clés de chiffrement contre la compromission ou la perte, ce qui pourrait entraîner la divulgation non autorisée ou la perte de données;
f) toutes les interfaces externes du service infonuagique sont cernées et protégées de manière appropriée;
g) les FSI documentent clairement les fonctions et les contrôles de sécurité mis en œuvre dans leurs services infonuagiques pour aider le gouvernement du Canada à comprendre les contrôles de sécurité qui relèvent de ses responsabilités. Ces contrôles comprennent ceux dont le FSI a hérité. Par exemple, un fournisseur de logiciels qui utilise un fournisseur d'infrastructure afin de livrer un SaaS hérite des contrôles de sécurité du fournisseur d'infrastructure. Dans ce cas, le fournisseur de services infonuagiques doit obtenir une assurance que l'IaaS ou la PaaS sous-jacente offerte pour le SaaS :
    - englobe dans sa portée les contrôles appropriés mis en œuvre;
    - a obtenu les certifications ou les rapports de vérification valides de tiers de l'industrie;
h) les ministères gèrent continuellement les vulnérabilités dans les systèmes informatiques. Ces mesures s'étendent aux FSI pour les composantes des services infonuagiques dans leur sphère de responsabilité;

[6] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html
[7] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776
[8] https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de

i) les FSI informent le gouvernement du Canada lorsqu'un incident sur le plan de la sécurité, une atteinte à la protection des données du gouvernement du Canada ou leurs services infonuagiques a des répercussions sur le service infonuagique du gouvernement. Ces avis doivent être envoyés :
   - aux personnes-ressources ministérielles compétentes (par exemple, le responsable du service infonuagique);
   - au Centre canadien pour la cybersécurité (CCC).

7.0 Conformité à l'Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI)

7.1 Orientation du SCT relative à la résidence des données électroniques (AMPTI 2017-02)

7.1.1 Dans l'esprit de l'Avis de mise en œuvre de la Politique sur la TI (AMPTI) 2017-02 du Secrétariat du Conseil du Trésor[9], on préfère que :

a) toutes les données électroniques sensibles classées **« Protégé A »** soient stockées dans une installation informatique approuvée par le gouvernement du Canada située à l'intérieur des frontières géographiques du Canada.
b) toutes les données électroniques du gouvernement du Canada de niveau « **Protégé A »** soient chiffrées lorsqu'elles sont transmises hors des zones de travail et des zones de sécurité contrôlées par le gouvernement du Canada au Canada ou à l'étranger.

8.0 Pratiques de codage sécurisé

8.1 L'entrepreneur doit respecter les pratiques exemplaires de l'industrie, y compris (sans s'y limiter) :

a) Pendant l'élaboration du code personnalisé nécessaire pour satisfaire au présent contrat :
   (i) L'entrepreneur accepte de désigner et de respecter un ensemble de lignes directrices régissant le codage sécurisé (comme les SAFECode Fundamental Practices for Secure Software Development[10]) lorsqu'il crée les produits à livrer mentionnés dans le contrat. Les lignes directrices doivent indiquer comment le code doit être formaté, structuré et commenté.
   (ii) L'entrepreneur accepte d'utiliser un ensemble d'interfaces communes de programmation des contrôles de sécurité (comme l'OWASP Enterprise Security API [ESAPI][11]). Les interfaces communes de programmation des contrôles de sécurité doivent définir comment les contrôles de sécurité doivent être appelés et comment ils doivent fonctionner.

[9] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-relative-residence-donnees-electroniques.html
[10] https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf
[11] https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

(iii) Tout code relatif à la sécurité doit faire l'objet d'un commentaire complet. Tout le code doit être examiné par au moins un autre entrepreneur en fonction des exigences de sécurité et des lignes directrices de codage avant qu'il ne soit considéré comme prêt pour l'essai unitaire.

(iv) Le logiciel ne doit comporter aucune des failles décrites dans la version actuelle du document OWASP Top Ten Web Application Security Risks[12].

(v) L'entrepreneur doit garantir que le logiciel ne contient aucun code ne servant pas à satisfaire à une exigence logicielle et affaiblissant la sécurité de l'application, y compris des virus informatiques, des vers, des bombes à retardement, des portes dérobées, des chevaux de Troie, des œufs de Pâques et toute autre forme de code malveillant.

(vi) L'entrepreneur doit faire l'analyse et la mise à l'essai de la sécurité de l'application pendant le cycle de vie de l'élaboration du système. L'entrepreneur doit transmettre ses constatations à AMC. L'entrepreneur doit éliminer toute défaillance au niveau de la sécurité découverte pendant la conception.

(vii) L'entrepreneur doit divulguer quels sont les outils utilisés dans l'environnement d'élaboration du logiciel afin d'encourager un codage sécurisé.

(viii) L'entrepreneur doit utiliser un système de contrôle des codes sources des logiciels qui authentifie et consigne les membres de l'équipe associés à tous les changements apportés au logiciel de base, ainsi qu'à tous les fichiers connexes de configuration et de construction.

(ix) L'entrepreneur doit utiliser un processus de construction qui crée de façon fiable une distribution complète à partir de la source. Ce processus doit comprendre une méthode permettant de vérifier l'intégrité du logiciel livré à AMC.

(x) L'entrepreneur doit divulguer tout logiciel d'un tiers utilisé dans le logiciel, y compris toutes les bibliothèques, les cadres, les composantes et autres produits, commerciaux, gratuits, libres ou non.

b) L'entrepreneur doit faire des efforts raisonnables pour s'assurer que les logiciels de tiers respectent toutes les exigences du présent accord et qu'ils sont aussi sécurisés que le code personnalisé élaboré en vertu de ce contrat.

9.0 Isolement des données

9.1 L'entrepreneur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources, afin que les données du gouvernement du Canada ne se retrouvent pas mêlées à celles d'autres locataires sans contrôle à cet effet, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système des services infonuagiques et de l'infrastructure de l'entrepreneur. Cela nécessite la mise en œuvre de

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

contrôles d'accès et la mise en place d'une séparation logique ou physique appropriée pour soutenir :

a) la séparation entre l'administration interne de l'entrepreneur et les ressources utilisées par ses clients;
b) la séparation des ressources des clients dans les environnements multilocataires afin d'empêcher que les activités d'un client malveillant ou compromis aient des répercussions sur le service ou les données d'un autre;
c) la capacité du gouvernement du Canada de soutenir l'isolement dans un environnement à locataires géré par le gouvernement du Canada.

9.2 À la demande du Canada, l'entrepreneur doit fournir au Canada un document qui décrit l'approche permettant d'assurer l'isolement voulu des ressources, de manière à ce que les données du Canada ne soient pas mêlées à celles d'un autre locataire pendant leur utilisation, stockage ou transit.

10.0 Gestion des clés

10.1 L'entrepreneur doit fournir au Canada un service de gestion des clés qui permet :

a) la création ou la génération et la suppression des clés de cryptage par le gouvernement du Canada;
b) la définition et l'application de politiques particulières qui contrôlent la manière dont les clés peuvent être utilisées;
c) la protection de l'accès au matériel relatif aux clés, y compris la prévention de l'accès par l'entrepreneur au matériel relatif aux clés de manière non chiffrée;
d) la capacité de vérifier tous les événements liés aux services de gestion des clés, y compris l'accès par l'entrepreneur, pour que le Canada puisse les examiner;
e) la capacité d'importer de façon sécuritaire les clés générées par le gouvernement du Canada à partir d'un module matériel de sécurité, géré sur place par le gouvernement du Canada, et ce, sans exposition du texte en clair des clés pendant le processus d'importation;
f) la capacité d'empêcher le fournisseur de services infonuagiques de récupérer des copies en texte clair des clés générées par le gouvernement du Canada;
g) la capacité de déléguer les privilèges liés à l'utilisation des clés pour leur usage par les services infonuagiques utilisés pour les services gérés par le gouvernement du Canada.

11.0 Gestion du risque de la chaîne d'approvisionnement

11.1 L'entrepreneur doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services infonuagiques. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.

12.0 Examen de la sécurité

12.1 Pendant l'élaboration du code personnalisé nécessaire pour satisfaire au présent contrat :

12.1.1 AMC a le droit de faire examiner le logiciel ou la solution pour confirmer l'absence de défauts de sécurité, à ses frais, à tout moment dans les 60 jours suivant la livraison[13]. L'entrepreneur s'engage à fournir un soutien raisonnable à l'équipe d'examen en fournissant le code source et l'accès aux environnements d'essai.

12.1.2 Les examens de la sécurité doivent couvrir tous les aspects du logiciel livré, y compris le code personnalisé, les composantes, les produits et la configuration du système.

12.1.3 Au minimum, l'examen de la sécurité doit couvrir toutes les exigences en matière de sécurité et devrait chercher toute autre vulnérabilité commune. L'examen peut comprendre une combinaison d'analyses de vulnérabilité, de tests d'intrusion, d'analyses statiques du code source et d'examen du code par des experts.

12.1.4 Les problèmes de sécurité découverts seront signalés à AMC et à l'entrepreneur. Tous les problèmes feront l'objet d'un suivi et ils seront résolus conformément à la section 13.0, *Gestion des problèmes de sécurité*.

13.0 Gestion des problèmes de sécurité

13.1 L'entrepreneur doit gérer les problèmes de sécurité comme suit.

13.1.1 L'entrepreneur doit faire le suivi de tous les problèmes de sécurité découverts pendant tout le cycle de vie, qu'il s'agisse de problèmes relatifs aux exigences, à la conception, à la mise en œuvre, aux essais, au déploiement ou à des questions opérationnelles. Le risque associé à chaque problème de sécurité sera évalué, documenté et communiqué à AMC dès que possible après sa découverte.

13.1.2 L'entrepreneur devra protéger adéquatement l'information concernant les questions de sécurité et la documentation connexe, afin d'aider à limiter la possibilité que les vulnérabilités dans le logiciel opérationnel soient exposées.

13.1.3 Les problèmes de sécurité repérés avant la livraison doivent être réglés par l'entrepreneur. Les problèmes de sécurité découverts après la livraison doivent être traités de la même manière que d'autres problèmes de sécurité, conformément aux exigences de la présente annexe technique sur la sécurité.

[13] Dans le présent document, la « livraison » est définie comme l'achèvement des modalités du contrat pour lequel une autorisation d'exploitation (AE) a été accordée par AMC, et le fournisseur de services infonuagiques (FSI) s'est engagé à respecter les conditions de l'AE et les échéanciers connexes, à la satisfaction d'AMC.

14.0 Assurance

14.1 L'entrepreneur doit fournir un « dossier de certification » composé de la documentation de sécurité créée tout au long du processus d'élaboration, de mise à l'essai et de mise en œuvre. Ce dossier de certification doit comprendre :

a) un plan de projet qui incorpore les activités d'évaluation et d'autorisation de sécurité (EAS) d'AMC (voir la section 15.0, *Évaluation et autorisation de sécurité [EAS]*);
b) la preuve de toute certification ou norme de vérification énumérée pour répondre aux exigences en matière de sécurité (voir la section 2.0, *Certifications*);
c) une matrice de traçabilité des exigences en matière de sécurité (MTES) (voir la section 3.0, *Exigences en matière de sécurité et traçabilité*);
d) une preuve des exigences liées au personnel (voir la section 4.0, *Exigences relatives au personnel*);
e) une preuve de la conformité aux exigences du Centre des opérations (voir la section 5.0, *Centres des opérations*);
f) une preuve de la conformité à toutes les politiques du gouvernement du Canada (AMOPS) (voir la section 6.0, *Conformité avec l'Avis de mise en œuvre de la Politique sur la sécurité [AMOPS]*), sous la forme d'une preuve d'une MTES ou d'un autre document convenable;
g) une preuve de la conformité à toutes les politiques du gouvernement du Canada (AMPTI) (voir la section 7.0, *Conformité à l'Avis de mise en œuvre de la Politique sur la technologie de l'information [AMPTI]*), sous la forme d'une preuve d'une MTES ou d'un autre document convenable;
h) une preuve des pratiques exemplaires de l'entrepreneur, y compris :
    (i) l'identification des lignes directrices de codage sécurisé utilisées pour tout code élaboré dans le cadre du présent contrat;
    (ii) l'identification de la source des interfaces de programmation des contrôles de sécurité;
    (iii) l'évaluation des vulnérabilités et les résultats, démontrant que la solution logicielle n'est pas susceptible à toutes les défaillances décrites dans le document *OWASP Top Ten Most Critical Web Application Vulnerabilities*;
i) les documents à livrer sur l'architecture et la conception (voir la section 15.0, *Évaluation et autorisation de sécurité [EAS]*), y compris :
    (i) la conception de haut niveau de la sécurité;
    (ii) la conception détaillée de la sécurité;
    (iii) le plan de mise à l'essai de la sécurité;
    (iv) le rapport de mise à l'essai de la sécurité;
    (v) le plan d'évaluation des vulnérabilités (ÉV);
    (vi) le rapport d'évaluation des vulnérabilités;
    (vii) le plan de vérification de l'installation de sécurité; et/ou
    (viii) le rapport de vérification de l'installation des composants de sécurité.

14.2 Le dossier doit établir que les exigences, la conception, la mise en œuvre et les résultats de la mise à l'essai de la sécurité ont été achevés correctement et que tous les problèmes de sécurité ont été résolus de manière appropriée.

14.3 L'architecte de la sécurité doit certifier que le logiciel répond aux exigences de sécurité, que toutes les activités de sécurité ont été effectuées et que tous les problèmes de sécurité repérés ont été documentés et résolus. Toute exception à l'état de la certification doit être pleinement justifiée dans un document au moment de la livraison.

14.4 Acceptation et maintenance de la sécurité

14.4.1 Acceptation

14.4.1.1 La solution ne sera pas acceptée tant que le dossier de certification de sécurité ne sera pas complet et que l'on aura obtenu l'assurance que toutes les données **« Protégé A »** seront protégées contre toute divulgation non autorisée susceptible de nuire sérieusement aux intérêts d'une personne, d'une entreprise ou d'un gouvernement.

14.4.1.2 Tout autre problème de sécurité qui n'a pas été résolu et qui ne menace pas la protection des données doit accompagner la documentation en vue d'une mise en œuvre ultérieure. AMC et l'entrepreneur conviennent de déployer les efforts nécessaires pour résoudre ces problèmes de sécurité additionnels et de négocier de bonne foi pour conclure une entente en vue d'exécuter les travaux requis pour les régler. AMC se réserve le droit de faire résoudre ces problèmes de sécurité en suspens, qui ne menacent pas la protection des données, à l'aide d'une autorisation de tâche (AT), si l'on détermine que la résolution du problème de sécurité exigerait une quantité de travail excessive.

14.4.2 Examen et résolution des problèmes de sécurité

14.4.2.1 Dans les 90 jours suivant l'obtention d'une autorisation d'exploitation (AE) d'AMC, si des problèmes de sécurité sont découverts ou soupçonnés raisonnablement, l'entrepreneur doit aider AMC à mener une enquête afin de déterminer la nature du problème. AMC et l'entrepreneur conviennent de déployer les efforts nécessaires pour résoudre les problèmes de sécurité et de négocier de bonne foi pour conclure une entente en vue d'exécuter les travaux requis pour les régler.

14.4.3 Autres problèmes de sécurité

14.4.3.1 L'entrepreneur doit déployer tous les efforts commercialement raisonnables compatibles avec de saines pratiques de développement de logiciels, en tenant compte de la gravité des risques, pour résoudre tous les problèmes de sécurité le plus rapidement possible.

15.0 Évaluation et autorisation de sécurité (EAS)

AMC a adapté le Processus d'application de la sécurité dans les systèmes d'information (PASSI), décrit dans la publication du CST, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*[14],

[14] https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie

comme base du processus d'évaluation et d'autorisation de sécurité (EAS). Le processus d'EAS est le mécanisme grâce auquel on comprend, atténue et gère, de façon uniforme et mesurable, le risque visant un système de TI, et ce, tout au long de son cycle de vie. Une autorisation d'exploitation (AE) est l'approbation donnée par un responsable opérationnel d'exploiter un projet, un programme, une installation ou un système selon certains paramètres (contrôles de sécurité) limitant le risque résiduel à un niveau jugé acceptable.

Le processus d'EAS d'AMC (décrit dans la présente section) est mené par **phases** visant à soutenir une philosophie de « sécurité intégrée à la conception ». Un point de révision suit chaque phase. Chacun des points de révision subséquents correspond à un niveau de détail croissant dans les phases d'architecture, de conception, de mise en œuvre et d'exploitation de la solution livrée. La revue sert à assurer la traçabilité en fonction des exigences de sécurité, la continuité dans la conception et une validation que les mécanismes de sécurité sont présents et adéquats.

15.1 L'entrepreneur doit se conformer aux exigences du processus d'EAS.

15.2 L'entrepreneur doit incorporer les phases du processus d'EAS d'AMC dans un échéancier de projet et obtenir l'approbation de cet échéancier du responsable du projet d'AMC avant d'entreprendre les travaux d'élaboration prévus au contrat.

15.3 L'entrepreneur doit respecter toutes les exigences énumérées à la section 15.5, *Exigences liées à l'évaluation et à l'autorisation de sécurité* à chaque phase du projet, conformément à l'échéancier de projet approuvé.

15.4 L'entrepreneur doit livrer tous les produits énumérés à la section 15.5, *Exigences liées à l'évaluation et à l'autorisation de sécurité* afin qu'ils soient examinés et approuvés par le responsable du projet d'AMC, et ce, avant de passer à la prochaine phase de l'élaboration.

15.5 Exigences liées à l'évaluation et à l'autorisation de sécurité

Les exigences pour chacune des phases du processus d'EAS sont décrites ci-dessous.

15.5.1 Exigences de la phase 1 de l'évaluation et de l'autorisation de sécurité (conception de haut niveau de la sécurité)

Le **point de révision de la phase 1** est établi après l'achèvement des éléments ci-dessous.

15.5.1.1 L'entrepreneur doit fournir un plan général de la conception de la sécurité qui comprend ce qui suit :

a) un schéma général des composants qui illustre clairement l'architecture globale et la répartition des services et des composants dans les zones de sécurité du réseau, et qui établit les principaux flux de données liés à la sécurité;
b) une description des mesures de défense du périmètre de la zone de sécurité du réseau;
c) une description de l'approche adoptée pour la séparation des données;
d) une description de la répartition de l'ensemble des exigences de sécurité technique au sein des éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture;

e) une description de la répartition de l'ensemble des exigences de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux;
f) une répartition des exigences de sécurité pour toutes les couches de l'architecture de la conception générale des services;
g) une définition des couches de l'architecture (p. ex. communication, virtualisation, plateforme ou système d'exploitation, gestion des données, intergiciels, applications opérationnelles);
h) une description de l'approche adoptée pour la gestion à distance;
i) une description de l'approche adoptée pour le contrôle d'accès;
j) une description de l'approche adoptée pour la gestion de la sécurité et la vérification;
k) une description de l'approche adoptée pour la gestion de la configuration;
l) une description de l'approche adoptée pour la gestion des correctifs;
m) une description de l'approche adoptée pour la suppression et le nettoyage des données du Canada;
n) un processus de mise hors service à suivre lorsque le système ne sera plus requis;
o) une justification des principales décisions concernant la conception.

15.5.1.2 L'entrepreneur doit fournir une matrice de traçabilité des exigences en matière de sécurité (MTES) qui contient les renseignements suivants pour chaque exigence en matière de sécurité figurant dans le **guide du SCT sur la MTES concernant les applications SaaS jusqu'au niveau « Protégé B »**, IB n° **14310732** :

a) le code d'identification des exigences en matière de sécurité (EMS);
b) l'énoncé des EMS;
c) une description suffisamment détaillée de la façon dont on répond à l'exigence en matière de sécurité dans la conception générale de la sécurité, afin de permettre au Canada de confirmer que les mesures de sécurité satisfont à cette exigence;
d) le titre des produits livrables prévus au contrat dans lequel l'entrepreneur présentera les détails de la solution de sécurité qu'il entend adopter pour répondre à l'exigence (p. ex. Plan de continuité du service).

15.5.2 Exigences de la phase 2 de l'évaluation et de l'autorisation de sécurité (conception détaillée de la sécurité)

Le **point de révision de la phase 2** est établi après l'achèvement des éléments ci-dessous.

15.5.2.1 L'entrepreneur doit fournir un plan détaillé de la conception de la sécurité qui comprend ce qui suit :

a) un schéma détaillé des composants (il doit s'agir d'une version approfondie du schéma général des composants);
b) une description de la répartition des mécanismes de sécurité technique au sein des éléments de la conception détaillée des services;
c) une description de la répartition des mécanismes de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux;
d) une justification des principales décisions concernant la conception.

15.5.2.2 L'entrepreneur doit fournir une matrice de traçabilité des exigences en matière de sécurité (MTES) qui contient les renseignements suivants pour chaque exigence en matière de sécurité figurant dans le **guide du SCT sur la MTES concernant les applications SaaS jusqu'au niveau « Protégé B »**, IB nº **14310732** :

a) le code d'identification des exigences en matière de sécurité (EMS);
b) l'énoncé des EMS;
c) une description suffisamment détaillée de la façon dont on répond à l'exigence en matière de sécurité dans la conception détaillée de la sécurité, afin de permettre au Canada de confirmer que les mesures de sécurité satisfont à cette exigence;
d) le titre des produits livrables prévus au contrat dans lequel l'entrepreneur présentera les détails de la solution de sécurité qu'il entend adopter pour répondre à l'exigence (p. ex. Plan de continuité du service).

15.5.3 Exigences de la phase 3 de l'évaluation et de l'autorisation de sécurité (mise en œuvre)

Le **point de révision de la phase 3** est établi après l'achèvement des éléments ci-dessous.

15.5.3.1 L'entrepreneur doit fournir un plan d'essai de la sécurité qui comprend ce qui suit :

a) les fonctions de sécurité faisant l'objet d'essais;
b) les éléments devant faire l'objet d'essais pour chaque fonction de sécurité ou ensemble de fonctions de sécurité, y compris :
   (i) une description du scénario ou de la procédure d'essai;
   (ii) les exigences environnementales;
   (iii) les liens de dépendance;
   (iv) les résultats attendus (c.-à-d. des critères de type réussite/échec).

15.5.3.2 L'entrepreneur doit présenter au Canada une matrice de traçabilité des exigences en matière de sécurité mise à jour qui contient des liens (des renvois à des éléments identifiables) vers les scénarios d'essai de sécurité pour chaque exigence faisant l'objet d'une mise à l'essai dans le cadre du plan d'essai de la sécurité.

15.5.3.3 L'entrepreneur doit fournir un plan d'évaluation des vulnérabilités qui comprend ce qui suit :

a) une description de la portée de l'évaluation des vulnérabilités;
b) une description du processus d'évaluation des vulnérabilités;
c) une description des outils qui serviront à évaluer les vulnérabilités, y compris le numéro de version des divers logiciels employés.

15.5.3.4 L'entrepreneur doit fournir un plan de vérification de l'installation des composants de sécurité qui comprend ce qui suit :

a) la méthode adoptée pour vérifier la sécurité;
b) un aperçu des composants faisant l'objet d'une vérification de la sécurité;
c) pour chaque composant faisant l'objet d'une vérification de la sécurité :
   (i) une description du scénario de vérification;
   (ii) les liens de dépendance;

(iii) les résultats escomptés (c.-à-d. des critères de type réussite/échec).

15.5.3.5 L'entrepreneur doit vérifier l'installation des composants de sécurité conformément au plan de vérification de l'installation des composants de sécurité.

15.5.3.6 L'entrepreneur doit présenter au Canada une matrice de traçabilité des exigences en matière de sécurité mise à jour qui contient des liens (des renvois à des éléments identifiables) vers les scénarios de vérification de l'installation des composants de sécurité pour chaque exigence faisant l'objet d'une mise à l'essai dans le cadre du plan de vérification de l'installation des composants de sécurité.

15.5.3.7 L'entrepreneur doit corriger les erreurs et omissions ayant trait à l'installation ou à la configuration relevées dans le cadre de la vérification de l'installation des composants de sécurité.

15.5.3.8 Le rapport de vérification de l'installation des composants de sécurité doit comprendre, pour chacun des éléments mis à l'essai compris dans le plan de vérification de l'installation des composants de sécurité :

a) les résultats escomptés;
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

15.5.3.9 L'entrepreneur doit réaliser des essais de sécurité conformément au plan d'essai de la sécurité.

15.5.3.10 Le rapport sur les essais de sécurité doit comprendre, pour chacun des éléments mis à l'essai dans le cadre du plan d'essai de la sécurité :

a) les résultats attendus (c.-à-d. des critères de type réussite/échec);
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

15.5.3.11 L'entrepreneur doit réaliser des évaluations des vulnérabilités conformément au plan d'évaluation des vulnérabilités et produire un rapport d'évaluation des vulnérabilités.

15.5.3.12 Le rapport d'évaluation des vulnérabilités doit comprendre ce qui suit :

a) une liste des résultats de l'évaluation des vulnérabilités;
b) pour chacune des vulnérabilités détectées :
    (i) une évaluation de la gravité de la vulnérabilité (p. ex. Common Vulnerability Scoring System [CVSS][15]);
    (ii) une description de la mesure corrective ou du correctif qui a été mis en œuvre pour résoudre la vulnérabilité;
c) pour toute vulnérabilité non résolue :
    (i) une évaluation de l'importance de la vulnérabilité;

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

(ii) la raison pour laquelle une mesure corrective ou un correctif n'a pas été mis en œuvre.

15.5.3.13 L'entrepreneur doit apporter des correctifs et prendre les mesures correctives nécessaires dans le cadre d'une activité d'évaluation des vulnérabilités.

ANNEXE E INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

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

a. Carte d'acquisition Visa ;

b. Carte d'acquisition MasterCard ;

c. Dépôt direct (national et international) ;

d. Échange de données informatisées (EDI) ;

e. Virement bancaire (international seulement) ;

f. Système de transfert de paiements de grande valeur (STPGV) (plus de 25 millions de dollars).

ANNEXE 4.1 – CRITÈRES D'ÉVALUATION DES SOUMISSIONS

1.1 Critères techniques

a) Nous recommandons au soumissionnaire de joindre à sa proposition une grille de correspondance entre les déclarations de conformité et les données justificatives que contient sa proposition.

Remarque. La grille de conformité en soi ne constitue pas une preuve démontrée. Le soumissionnaire doit soumettre le curriculum vitae détaillé de chacune des ressources proposées.

b) Les programmes d'études doivent avoir été suivis dans une université, un collège ou une école secondaire canadiens reconnus* ou un établissement équivalent, comme l'a établi un organisme canadien reconnu d'évaluation des diplômes* si le diplôme a été obtenu à l'extérieur du Canada.

* Vous trouverez la liste des établissements offrant un service d'évaluation des diplômes sur le site du Centre d'information canadien sur les diplômes internationaux à l'adresse https://www.cicdi.ca/1/accueil.canada.

Afin d'obtenir des points pour les attestations d'études et les attestations professionnelles, le soumissionnaire doit joindre une copie des diplômes à sa proposition. Sinon, il devra les fournir sur demande et dans le délai imparti par l'autorité contractante.

c) Le soumissionnaire doit savoir que la simple énumération de l'expérience sans données justificatives décrivant où et comment cette expérience a été acquise ne représente pas une « preuve » pour les besoins de l'évaluation.

Chaque sommaire de projet doit comprendre le nom, le numéro de téléphone ou l'adresse électronique de la référence du client. Le Canada se réserve le droit de demander des références de clients et de communiquer avec ces derniers pour valider les renseignements fournis dans la proposition.

Le soumissionnaire doit fournir des renseignements complets indiquant où, quand (mois et année) et comment (par quelles activités et responsabilités) les compétences et l'expérience mentionnées ont été acquises. L'expérience acquise au cours des études n'est pas considérée de l'expérience professionnelle. Toute l'expérience professionnelle doit avoir été acquise dans un véritable milieu de travail et non dans le cadre d'un programme d'études. Les stages de programmes coopératifs sont assimilés à des expériences de travail, à condition de correspondre aux services requis.

Le soumissionnaire est aussi prié de noter que les mois d'expérience acquise dans le cadre d'un projet pour lequel l'échéancier chevauche celui d'un autre projet cité en référence ne sont comptés qu'une seule fois. Par exemple, si la période du projet 1 va de juillet 2001 à décembre 2001 et que la période du projet 2 est d'octobre 2001 à janvier 2002, le nombre total de mois d'expérience pour ces deux références de projet est de sept (7) mois. Le soumissionnaire doit indiquer dans les curriculum vitæ le nombre de mois ou d'années comptés pour chaque projet.

Pour chaque critère, le soumissionnaire doit fournir des détails sur les qualifications, l'expérience pertinente et l'expertise des ressources proposées. Dans le cas des critères obligatoires et cotés, l'expérience des ressources proposées doit être clairement exposée au moyen du sommaire ou de la description des projets auxquels elles ont déjà travaillé, et il faut indiquer les dates où le travail a été exécuté et le client. De plus, la matrice des critères d'évaluation doit être utilisée pour répondre aux critères obligatoires et cotés. Par conséquent, les réponses doivent être directement inscrites dans la matrice, avec une explication de la manière dont chaque critère est rempli et des renvois aux pages et aux numéros des projets indiqués dans le curriculum vitæ.

d) Il est recommandé que le soumissionnaire inclue également dans le curriculum vitæ la cote de sécurité actuelle des ressources proposées, ainsi que le numéro de dossier de la Direction de la sécurité industrielle canadienne (DSIC) correspondant.

e) Une vérification des références et des entrevues peuvent être réalisées. Si le Canada procède à celle-ci, il doit envoyer des courriels aux personnes citées en référence par le soumissionnaire (sauf si la personne citée en référence ne peut être jointe qu'au téléphone). Le Canada doit acheminer les demandes par courriel le même jour aux personnes désignées par tous les soumissionnaires. Le Canada n'attribue aucun point s'il n'a pas reçu les réponses dans un délai de cinq (5) jours ouvrables. S'il y a contradiction entre l'information donnée par la personne de référence et celle fournie par le soumissionnaire, seule la première est évaluée. Aucun point n'est accordé si la personne donnée en référence n'est pas un client du soumissionnaire (c.-à-d., le client de référence ne peut pas être un client d'un affilié du soumissionnaire). De même, aucun point n'est accordé si le client est lui-même un affilié ou une autre entité qui entretient des liens de dépendance avec le soumissionnaire. Des références de l'État sont permises.

Les sommaires de projet et de contrat attribués doivent comprendre les renseignements suivants :

- le nom de l'organisation cliente;
- les dates de début et de fin du contrat (du JJ/MM/AAAA au JJ/MM/AAAA);
- la valeur monétaire du projet (en dollars canadiens);
- une brève description des services fournis (y compris les rôles assumés et les activités réalisées par la ressource proposée) :
    - les renseignements de référence du client doivent comprendre le nom, le titre, le numéro de téléphone et l'adresse électronique du projet du client ou de l'autorité technique.

À moins d'indication contraire, chaque projet doit être d'une durée d'au moins quatre (4) mois pour être pris en compte.

Définitions

- **Intervenants**. Personne ou organisation qui influe ou a influé sur les objectifs et les résultats d'un projet, qui prend ou a pris part à la réalisation ou à la supervision du projet et dont les intérêts peuvent être affectés par l'exécution ou l'achèvement du projet.
- **Organisation ou agence du gouvernement fédéral**. Doit figurer à l'annexe I, II, III, V ou VI (partie 1) de la *Loi sur la gestion des finances publiques* (accès en ligne à l'adresse https://laws-lois.justice.gc.ca/fra/lois/f-11/index.html.)
- **Haute direction**. Composée du président-directeur général (PDG), du dirigeant principal de l'information (DPI), du sous-ministre adjoint (SMA), du vice-président, du chef de l'exploitation et du dirigeant principal des finances (DPF). Dans le secteur privé, la haute direction est composée d'un président, d'un vice-président et d'un président-directeur général (PDG).
- **National**. Niveau ayant une incidence sur les opérations dans au mins quatre (4) provinces ou territoires.
- **Projet important**. Projet ou programme qui répond aux critères suivants :
    - couvre plusieurs programmes ou services auxquels prend part au moins une organisation ou une agence du gouvernement fédéral externe ou une entreprise du secteur privé;
    - a une durée d'au moins 12 mois;
    - dispose d'une équipe comptant plus de 45 personnes (employés et entrepreneurs);
    - appuie un organisme de plus de 1 000 employés.
- **Secteur public**. Nom qui désigne des organismes du gouvernement fédéral (y compris les sociétés d'État), des gouvernements provinciaux, des administrations municipales ainsi et de toute organisation quasi gouvernementale au Canada.

- **Grande organisation publique**. Toute administration du secteur public – fédérale, provinciale ou municipale – dont les activités se concentrent sur des services offerts à l'ensemble de la population, dont l'éducation, la sécurité sociale, la justice et les services de santé.

1.2 Critères obligatoires

La soumission doit remplir tous les critères techniques obligatoires précisés dans la présente section. Une soumission conforme est évaluée et notée selon les critères précisés dans les tableaux ci-dessous. Le soumissionnaire doit fournir la documentation nécessaire pour faire la preuve qu'il satisfait aux différentes exigences.

Une soumission qui ne répond pas à tous les critères techniques obligatoires est jugée irrecevable. La conformité à chaque critère technique obligatoire doit être démontrée séparément.

N°	CRITÈRE OBLIGATOIRE	RESPECTÉ / NON RESPECTÉ	RENVOI À LA SOUMISSION
	Exigences opérationnelles		
O1	Le soumissionnaire doit proposer une plateforme de communication à canaux multiples de type SaaS qui permet aux Canadiens et aux Canadiennes en détresse à l'étranger de communiquer avec le CISU en utilisant des canaux de communication modernes. Il doit démontrer que la plateforme : • intègre au moins les canaux de communication suivants : messagerie instantanée (SMS), application WhatsApp et clavardage en direct; • est en mesure d'intégrer et d'abandonner de nouveaux canaux en réponse à l'évolution des modes d'utilisation des médias sociaux et les applications de clavardage; • permet 30 connexions simultanées.		
O2	Le soumissionnaire doit démontrer que la plateforme : • incorpore toutes les communications dans un seul centre de mobilisation; • incorpore des outils d'automatisation du flux de travail, tels que des messages de réponse préautorisés, des messages de réponse automatisés, l'acheminement des messages, etc.; • a la capacité d'exporter des données de conversation.		
O3	Le soumissionnaire doit confirmer que sa plateforme : • est offerte selon le modèle SaaS; • prends en charge plusieurs langues, dont l'anglais et le français; • permet l'intégration d'applications de tiers, notamment avec Microsoft Dynamics 365; • dispose d'un cadre souple permettant la conservation et l'élimination des données et qui peut être harmonisé avec les exigences d'AMC; • fonctionne avec un haut niveau de disponibilité et les mécanismes de redondance des centres de données; • traite et stocke toute les données au Canada; • fournit un soutien technique ininterrompu aux agents des centres de contact.		
O4	Le soumissionnaire doit démontrer que sa plateforme : • répond aux normes de sécurité technique établies à l'annexe D (qui porte sur les exigences techniques en matière de sécurité informatique), notamment : ○ ISO/IEC 27001:2013 (ou ISO 27001),		

	○ AICPA SOC 2, type II; • assure la gestion de comptes et offre des fonctionnalités de vérification détaillées.		
O5	Le responsable du projet doit fournir des détails sur le plan de mise en œuvre du projet, y compris les noms et les biographies des membres de l'équipe de mise en œuvre, ainsi qu'un aperçu du plan de mise en œuvre.		

Remarque. Le soumissionnaire retenu s'engage à travailler avec le personnel de la sécurité informatique d'AMC afin de mener à bien un processus interne d'évaluation de la sécurité et d'autorisation défini à l'annexe D (qui porte sur les exigences techniques en matière de sécurité informatique) et en particulier, de compléter les documents répertoriés à la section 14.

2.0 Critères cotés

Les propositions sont évaluées et cotées conformément aux critères d'évaluation énoncés dans la présente section.

N°	CRITÈRE COTÉ	NOTE MAX.	BARÈME	RÉPONSE DU SOUMISSIONNAIRE ET EXPÉRIENCE DÉMONTRÉE
Capacité de plateforme				
C1	Communication simultanée avec plusieurs clients en utilisant de multiples canaux de communication. L'interface utilisateur doit être simple et intuitive, et créer un environnement opérationnel pour les agents qui facilite des flux de travail efficaces et efficients.	10	Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise. L'information est claire et détaillée. Des exemples portant sur des projets antérieurs ont été fournis. 10 points. Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise, mais comporte un élément mal défini dans la soumission. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou comporte plus d'un élément mal défini dans la soumission. 0 point.	
C2	Utilisation d'un robot conversationnel qui peut être appliqué à tous les canaux de communication intégrés, globalement ou selon des règles de routage, et qui utilise le traitement du langage naturel afin d'assurer une compréhension contextuelle. Le robot conversationnel doit être offert en anglais et en français.	10	Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise. L'information est claire et détaillée. Des exemples portant sur des projets antérieurs ont été fournis. 10 points. Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise, mais comporte un élément mal défini dans la soumission. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou comporte plus d'un élément	

			mal défini dans la soumission. 0 point.	
C3	Fourniture d'une variété d'outils d'analyse de données et de production de rapports personnalisés et prédéfinis.	10	Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise. L'information est claire et détaillée. Des exemples portant sur des projets antérieurs ont été fournis. 10 points. Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise, mais comporte un élément mal défini dans la soumission. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou comporte plus d'un élément mal défini dans la soumission. 0 point.	
C4	Configuration de l'interface de clavardage en direct en vue de l'intégrer aux sites Web d'AMC. Le soumissionnaire doit démontrer que l'interface client du clavardage en direct est offerte en anglais et en français.	10	Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise. L'information est claire et détaillée. Des exemples portant sur des projets antérieurs ont été fournis. 10 points. Le soumissionnaire a démontré que sa plateforme en ligne présente la capacité requise, mais comporte un élément mal défini dans la soumission. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou comporte plus d'un élément mal défini dans la soumission. 0 point.	
Note de passage : 30 points			**Note :**	

N°	**CRITÈRE COTÉ**	**NOTE MAX.**	**BARÈME**	**RÉPONSE DU SOUMISSIONNAIRE ET EXPÉRIENCE DÉMONTRÉE**
Formation et soutien technique : Le soumissionnaire doit démontrer les méthodes et le niveau d'expérience en ce qui concerne leur plateforme de communication à canaux multiples au cours des trois (3) dernières années précédant la date de clôture de la présente demande de propositions, pour ce qui est des éléments ci-dessous.				
C5	Formation à distance ou en personne pour les petits groupes.	10	Le soumissionnaire a démontré qu'il possède la capacité requise à l'interne. L'information est claire et détaillée. Le soumissionnaire a démontré qu'il a acquis au moins deux (2) ans d'expérience au cours des trois (3) dernières années.	

			10 points. Le soumissionnaire a démontré qu'il possède la capacité requise à l'interne, mais un élément demeure mal défini dans la soumission. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou comporte plus d'un élément peu clair dans la soumission. 0 point.	
C6	Soutien pour aider les agents qui éprouvent des difficultés à naviguer dans la plateforme.	10	Le soumissionnaire a démontré qu'il possède la capacité requise à l'interne. L'information est claire et détaillée. Le soumissionnaire a démontré qu'il possède au moins 2 ans d'expérience au cours des trois dernières années. 10 points. Le soumissionnaire a démontré qu'il possède la capacité requise à l'interne, mais un élément demeure peu clair. 7 points. La plateforme proposée du soumissionnaire n'a pas la capacité requise ou il y a plus d'un élément peu clair dans la soumission. 0 point.	
C7	Méthodes de formation comme les décrit l'Énoncé des travaux.	10	Les méthodes de formation abordent et démontrent le fait que le soumissionnaire a la capacité de fournir la formation requise décrite dans l'Énoncé des travaux et est en outre appuyé par des outils de formation en ligne en personne et la disponibilité d'un soutien technique pendant les heures de travail. 10 points. Les méthodes de formation abordent et démontrent le fait que le fournisseur a la capacité de fournir la formation requise décrite dans l'Énoncé des travaux, mais elles comportent un élément mal défini. 7 points. La plateforme proposée du	

			soumissionnaire n’a pas la capacité requise ou comporte plus d’un élément mal défini dans la soumission. 0 point.	
C8	Soutien technique comme le décrit l’Énoncé des travaux.	10	Le soutien technique aborde et démontre le fait que le soumissionnaire a la capacité de fournir un accès téléphonique à son personnel de soutien technique en tout temps (24 heures sur 24, 7 jours sur 7). 10 points. Le soutien technique aborde et démontre le fait que le soumissionnaire a la capacité d’offrir un accès téléphonique à son personnel de soutien technique pendant les heures de bureau, comme le décrit l’Énoncé des travaux, mais peut comporter un élément mal défini. 7 points. La plateforme proposée du soumissionnaire n’a pas la capacité requise ou comporte plus d’un élément mal défini dans la soumission. 0 point.	
Note de passage : 30 points			**Note :**	

Démonstration

Avant l'attribution du contrat, le soumissionnaire peut être appelé à faire une démonstration de leur système pour faire la preuve que celui-ci satisfait à toutes les exigences précisées dans l'Énoncé des travaux et valider les exigences opérationnelles. Le Canada se réserve le droit de déclarer une soumission irrecevable si l'équipe d'évaluation des soumissions détermine que le soumissionnaire n'a pas réussi à démontrer sa capacité technique à répondre aux exigences.

La démonstration doit être réalisée virtuellement et sans la contribution financière du Canada. La démonstration ne doit pas durer plus d'une (1) heure.

Le Canada doit informer le soumissionnaire de la date prévue de la démonstration au moins cinq (5) jours ouvrables à l'avance.