Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.,/11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Title - Sujet National Cybercrime Solution Projec Solution nationale en matière de cybercriminalité	
Solicitation No. - N° de l'invitation M7594-205915/D	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client M7594-205915	**Date** 2021-05-03
GETS Reference No. - N° de référence de SEAG PW-$$XL-155-39352	
File No. - N° de dossier 155xl.M7594-205915	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-06-22 Heure Avancée de l'Est HAE

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

Address Enquiries to: - Adresser toutes questions à: Labossière, Jean-Claude	**Buyer Id - Id de l'acheteur** 155xl
Telephone No. - N° de téléphone (613) 858-7359 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

Le modification 002 de l'ìnvitation à:

1. Modifier la date de clôture de la demande de soumissions.
2. Modifier la section 5.0 énonce de travaux; paragraphe 5.1.1 Annexe A
3. Modifier La section 4.0, paragraphe a) iii**,** Appendice B à l'Annexe C Obligations en matière de sécurité
4. soumissionner vise à publier les questions et réponses.

1.0) La date de clôture de la demande de soumissions est REPORTÉE au 25 Mai 2021, à 14h00 **(HNE) pour le 22 Juin 2021 à 14h00 (HNE).**

2.0) La section 5.0 énonce de travaux; paragraphe 5.1.1 - Annexe A est SUPPRIMÉE et REMPLACÉE par:

5. Plan de sécurité du système

a) L'entrepreneur doit examiner toutes les exigences de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité (MTES) et y répondre; il doit proposer un mécanisme pour répondre à l'exigence. En cas de conflit entre les exigences de l'ensemble de la DP et la MTES, la MTES aura préséance.

b) L'entrepreneur doit aborder tous les risques cernés par les processus de conformité du gouvernement du Canada, comme les vérifications, les activités liées à l'évaluation et autorisation de sécurité (EAS), les évaluations de la menace et des risques (EMR) et les évaluations des facteurs relatifs à la vie privée (EFVP).

c) L'entrepreneur doit permettre au gouvernement du Canada où à ses délégués, sans frais pour le gouvernement du Canada, d'accéder aux environnements de développement et d'essai au sein de l'espace infonuagique Protégé B de la GRC pour inspecter et vérifier la conformité de l'entrepreneur avec les exigences prévues au contrat en matière de confidentialité, de sécurité et de gestion de l'information, et d'avoir pleinement accès à l'ensemble des dossiers et renseignements personnels.

d) La solution doit permettre au gouvernement du Canada d'installer des prises d'accès réseau passives pour une capture réseau complète et soutenue de tout le trafic réseau de la couche IP (protocole Internet) et des interactions entre les composantes de la SNC avec la possibilité d'inspecter les données chiffrées.

e) L'entrepreneur doit collaborer aux inspections et aux vérifications de sécurité demandées par le gouvernement du Canada et fournir les preuves suivantes :

i) les documents sur le flux de données et la description de la protection, de l'architecture et de la sécurité des données, pour ce qui a trait aux travaux prévus au contrat;

ii) les plans de gestion des risques, les évaluations des risques et les EFVP propres à l'entrepreneur, pour ce qui a trait aux travaux prévus au contrat;

iii) les entrevues des employés de l'entrepreneur et de tiers conseillers menées par le gouvernement du Canada au cours des heures de travail normales, ou bien en dehors de ces heures selon une entente mutuelle.

5.1 Exigences générales en matière de conformité

a) La SNC doit être protégée et sécurisée conformément aux politiques et aux lois du gouvernement du Canada en matière de sécurité. L'entrepreneur doit assurer la sécurité de la SNC conformément aux exigences en matière de sécurité continue ci-après.

5.1.1 Conformité aux politiques du gouvernement du Canada

a) L'entrepreneur doit se conformer aux politiques et aux lois en matière de sécurité suivantes du gouvernement du Canada concernant le transport et la transmission des renseignements « Protégé B ».

Transport/transmission : L'échange physique de renseignements de nature délicate doit respecter les modalités du contrat. Lorsqu'un service de livraison est utilisé, il doit fournir une preuve d'expédition, un suivi pendant l'expédition et une attestation à la livraison.

Transport	Transport : la transmission de renseignements et de biens de nature délicate d'une personne ou d'un lieu à un autre par l'entremise d'une personne qui a besoin de connaître les renseignements ou besoin d'accéder au bien.
Transmission	Transmission : la transmission de renseignements et de biens de nature délicate d'une personne ou d'un lieu à un autre par l'entremise d'une personne qui n'a pas besoin de connaître les renseignements ou d'accéder au bien.

Remarque :

1. Pour le transport de renseignements « Protégé B » (déplacement en direction ou à partir d'un endroit tiers en vue d'une rencontre ou d'une entrevue) : Il est possible d'utiliser une valise ou un autre contenant de solidité égale ou supérieure au lieu d'une enveloppe. Insérer dans un emballage ou une enveloppe double les biens fragiles, lourds, encombrants ou volumineux pour les protéger.
2. Pour la transmission de renseignements « Protégé B » (par Postes Canada ou courrier recommandé) : Adresser de façon non spécifique. Ajouter « À n'être ouvert que par » lorsqu'il convient d'appliquer les principes du besoin de savoir ou d'accéder.

5.1.2 Examen et certifications par des tiers

a) L'entrepreneur doit posséder des certifications valides et à jour de l'industrie du début à la fin du contrat :

i) Norme ISO/IEC 27001:2013 Technologies de l'information – techniques de sécurité – exigences en matière de systèmes de gestion de la sécurité de l'information ;

ii) Norme ISO/IEC 27017:2015 Technologies de l'information – techniques de sécurité – code de pratique pour les contrôles de sécurité de l'information fondée sur la norme ISO/IEC 27002:2013 Technologies de l'information – techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information des services infonuagiques;

iii) Norme ISO/IEC 27018:2019 Technologies de l'information – techniques de sécurité – code de pratique pour la protection des renseignements permettant d'identifier une personne (RIP) dans les services infonuagiques publics utilisés comme processeur de RIP ;

iv) Rapport Service Organization Control (SOC) 2 Type II de l'AICPA pour les principes de confiance associés à la sécurité, à la disponibilité, à l'intégrité du traitement, à la protection des renseignements personnels et à la confidentialité, préparé par un comptable agréé indépendant.

b) Chaque rapport de certification ou de vérification fourni doit : (i) mentionner le nom légal de l'entreprise de l'entrepreneur ou du sous-processeur applicable; (ii) mentionner la date de certification de l'entrepreneur ou du sous-processus et l'état de cette certification; et (iii) dresser la liste des services visés par le rapport de certification. Si la méthode détachée est utilisée pour exclure des fournisseurs de sous-services (p. ex. service d'hébergement de données), le rapport d'évaluation du fournisseur de sous-services doit être inclus.

c) Chaque vérification doit faire l'objet d'un rapport à la disposition du Canada. Les certifications doivent être prouvées au moyen de pièces justificatives (p ex. rapport d'évaluation ISO préparé pour valider la conformité avec les normes ISO), et les rapports du vérificateur doivent contenir toute observation concrète. L'entrepreneur doit régler rapidement tout problème soulevé dans un rapport de vérification, à la satisfaction du vérificateur.

d) Tout rapport de vérification SOC 2 Type II doit être préparé dans les 12 mois précédant la date de début des opérations. Une lettre spéciale peut être fournie pour montrer que l'entrepreneur attend son renouvellement, s'il y a un écart entre la date du rapport du fournisseur de services et la fin de l'exercice de l'organisation utilisatrice (année civile ou fiscale)

e) L'entrepreneur doit conserver ses certifications ISO 27001, ISO 27017, ISO 27018 et SOC 2 Type II du début à la fin du contrat et fournir annuellement ou rapidement, à la demande du Canada, tous les rapports et les dossiers qu'il pourrait être raisonnable d'exiger en vue de démontrer que ses certifications sont valides et à jour.

5.1.3 Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques

a) Si, durant le contrat et après l'approbation de l'autorité responsable du projet, l'entrepreneur fait migrer l'application ou des données d'un lieu physique à une solution infonuagique, il doit démontrer que le fournisseur de services infonuagiques :

i) satisfait aux exigences en matière de sécurité énoncées dans le Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage qui visent les services infonuagiques utilisés pour la SNC;

ii) a fait l'objet d'une évaluation dans le cadre du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques du Centre canadien pour la cybersécurité (ITSM.50.100) .

b) Tout fournisseur de services infonuagiques qui a participé au processus doit confirmer au moyen de documents qu'il a terminé le processus d'évaluation, soit : (i) une copie du dernier rapport d'évaluation fourni par le CCCS; ou (ii) une copie du dernier résumé de rapport fourni par le CCCS.

5.1.4 Gestion des risques liés à la chaîne d'approvisionnement

a) L'entrepreneur doit disposer de mesures de protection pour atténuer les risques et les vulnérabilités liés à la chaîne d'approvisionnement qui touchent les services de TI afin d'assurer la sécurité des systèmes d'information et des éléments de TI utilisés pour fournir les services. Cela inclut, sans s'y limiter, l'élaboration et la prise de mesures pour atténuer et contenir les risques associés à la sécurité des données par une séparation appropriée des tâches, un contrôle d'accès basé sur les rôles et des droits d'accès minimaux pour tout le personnel, y compris les sous-traitants de la chaîne d'approvisionnement.

b) L'entrepreneur doit tenir un plan de gestion des risques liés à la chaîne d'approvisionnement décrivant son approche à cet égard et la façon dont elle lui permet d'atténuer ces risques.

c) L'approche de gestion des risques liés à la chaîne d'approvisionnement doit être harmonisée avec une des pratiques exemplaires suivantes :

i) ISO/IEC 27 036 Technologies de l'information – techniques de sécurité – sécurité de l'information dans le contexte des relations avec les fournisseurs (partie 1 de 4);

ii) Publication spéciale de la NIST 800-161 – Pratiques de gestion des risques liés à la chaîne d'approvisionnement pour les organisations et les systèmes d'information fédéraux.

5.2 Examen de la conformité

a) Le Canada effectuera, chaque année, une vérification et un examen de la conformité approuvés par le gouvernement du Canada – payés par l'entrepreneur – qui comprennent, mais sans s'y limiter :

i) l'assurance que la solution est conforme aux exigences de sécurité de la SNC (voir l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité) et au profil de contrôle de sécurité ministériel (PCSM) de la GRC, y compris un examen du plan d'action et des jalons visant à s'assurer que les jalons sont atteints;

ii) l'assurance que tous les logiciels de la solution possèdent une version à jour et actuelle des mises à jour et des correctifs de sécurité pour toutes les vulnérabilités connues;

iii) la vérification que l'entrepreneur surveille de façon proactive les vulnérabilités des logiciels de la SNC et qu'il installe tout correctif de sécurité et toute nouvelle version des logiciels nécessaire à la correction de ces vulnérabilités;

iv) la composition de l'équipe de base de l'entrepreneur.

b) L'entrepreneur doit fournir les pièces justificatives requises dans les dix (10) jours ouvrables suivant une demande présentée par le gouvernement du Canada dans le cadre de l'examen de la conformité.

c) Si le Canada juge que les pièces justificatives ne démontrent pas le respect du contrat, il demandera à l'entrepreneur un plan dressant les mesures qu'il prendra pour régler les écarts relevés par rapport aux conditions générales du contrat.

5.3 Validation de sécurité

a) L'entrepreneur doit remettre au Canada une MTES offrant un suivi à l'égard de chaque exigence d'assurance de la sécurité de la SNC marquée aux fins de validation dans l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité. Pour chaque exigence, la MTES doit indiquer des renvois à des documents de conception des services, qui décrivent les mesures de sécurité à mettre en œuvre. La matrice permet de s'assurer que la conception générale des services répond pleinement aux exigences en matière de sécurité.

b) Il faut joindre à la MTES présentée au gouvernement du Canada tous les documents portant sur les services auxquels elle renvoie. Ceux-ci doivent décrire les mesures de sécurité avec suffisamment de détails pour permettre au gouvernement du Canada de confirmer qu'elles répondent aux exigences qui sont énoncées dans l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité de la SCN.

c) L'entrepreneur doit travailler en collaboration avec la GRC pour évaluer la solution par rapport au PCSM de la GRC dans le cadre du processus d'EAS.

5.4 Sécurité des systèmes et des données de l'environnement

5.4.1 Attestation de sécurité des installations

a) Tout au long des travaux, l'entrepreneur doit posséder une attestation de sécurité de niveau protégé B pour toutes les installations primaires, secondaires et de reprise après sinistre où sont hébergées, entreposées ou traitées des données de la SNC, conformément à la Directive sur la gestion de la sécurité du gouvernement du Canada .

5.4.1.1 Sécurité matérielle

a) L'entrepreneur doit maintenir des mesures de sécurité matérielle en vue de protéger les installations de TI et les systèmes d'information qui contiennent et traitent des données de la SNC des accès non autorisés, des altérations, des pertes, des dommages et des saisies, et ses mesures doivent être fondés sur une approche de la sécurité matérielle axée sur la prévention-détection-intervention-récupération. À tout le moins, l'approche doit inclure les éléments suivants :

i) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément au niveau de service prescrit;

ii) l'utilisation adéquate des supports de TI;

iii) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;

iv) le contrôle de l'accès aux dispositifs de sortie et d'entreposage des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;

v) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, validé par deux formes d'identification;

vi) l'escorte des visiteurs et la surveillance de leurs activités;

vii) la tenue de registres de vérification de l'accès physique;

viii) le contrôle et la gestion des dispositifs d'accès physique;

ix) l'application de mesures de protection des données de la SNC à d'autres lieux de travail (p. ex. les sites de télétravail);

x) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.

Source : Directive sur la gestion de la sécurité du gouvernement du Canada .

h) Les installations de l'entrepreneur doivent être dotées de mesures de protection physique appliquées conformément aux directives et aux normes en

matière de sécurité matérielle de la GRC, particulièrement le guide G1-025 – Protection, détection et intervention .

i) L'entrepreneur doit aviser l'autorité responsable du projet et la Direction des services de la sécurité du personnel (anciennement la DSIC) de toute amélioration ou modification apportée aux installations qui gèrent la SNC.

5.4.2 Zones de sécurité

a) L'entrepreneur doit utiliser des contrôles de sécurité afin d'assurer un isolement approprié des ressources, afin que les données de la SNC ne se retrouvent pas mêlées à celles d'autres locataires, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système du service. Cela comprend les contrôles d'accès et le renforcement des mesures d'isolement logique et physique afin d'assurer :

i) la séparation de l'administration interne de l'entrepreneur des ressources utilisées par ses clients;

ii) 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.

b) L'entrepreneur doit veiller à ce que les zones de sécurité du réseau soient toujours harmonisées avec :

i) les Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du Centre de la sécurité des télécommunications (CST) ;

ii) les Considérations de conception relatives au positionnement des services dans les zones (ITSG-38) du CST .

c) L'entrepreneur doit veiller à la surveillance et à la maintenance des zones de sécurité du réseau pour :

i) Assurer un contrôle rigoureux de toutes les interfaces des zones publiques, y compris tous les réseaux externes non contrôlés comme Internet, à un périmètre de sécurité déterminé;

ii) appliquer des mesures de protection et de défense périmétrique (p. ex. pare-feu, routeurs) pour intercepter tout le trafic et protéger les serveurs qui sont accessibles par Internet.

d) Du début à la fin du contrat, tout changement prévu ou non prévu à l'environnement doit être documenté et faire l'objet d'une mise à jour, conformément au plan de gestion du changement et aux processus connexes.

5.4.3 Examen de la conception des services

a) La conception des services pour la SNC doit être examinée et approuvée par le Canada. L'entrepreneur doit notamment fournir au Canada une copie de l'architecture proposée pour la SNC, qui permettra au Canada d'examiner :

i) les mesures de protection et de sécurité et les éléments de sécurité proposés qui seront appliqués dans le cadre de la SNC;

ii) la configuration et la fiabilité de tous les dispositifs de sécurité.

5.4.4 Protection contre les maliciels

a) L'entrepreneur doit protéger des cyberattaques les éléments de TI utilisés pour mettre en application et gérer la solution, notamment en surveillant les dispositifs, les serveurs, les périphériques et les postes de travail, ainsi qu'empêcher toute source externe d'y pénétrer.

b) La protection du réseau est nécessaire et elle doit être maintenue afin de pouvoir détecter et éliminer les logiciels malveillants ou les tentatives de connexion au réseau qui proviennent de l'extérieur et qui ne sont pas autorisées.

c) L'entrepreneur doit procéder au balayage de l'environnement hébergeant la SNC afin de détecter la présence de maliciels. Des mécanismes actifs de protection de l'hôte doivent être intégrés aux serveurs qui effectuent :

i) le balayage de maliciels à l'accès;

ii) le balayage actif et périodique de maliciels au moins une fois par mois.

5.4.5 Mises à jour de sécurité

a) L'entrepreneur doit effectuer les mises à jour de sécurité des systèmes d'exploitation et des applications afin de corriger les vulnérabilités au moyen d'une approche axée sur les risques et harmonisée avec la méthode figurant dans le document Correction des systèmes d'exploitation et des applications – Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSB-96) du Centre de la sécurité des télécommunications .

5.4.6 Gestion des correctifs et des vulnérabilités

a) Pour gérer les correctifs, l'entrepreneur doit au moins effectuer ce qui suit :

i) s'assurer qu'une version prise en charge et à jour des applications et des systèmes d'exploitation est utilisée;

ii) veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement;

iii) établir l'ordre de priorité des correctifs et des ensembles de modifications provisoires critiques à l'aide d'une approche fondée sur le risque;

iv) faire des mises à l'essai et des vérifications pour s'assurer que les correctifs ont été appliqués correctement.

5.4.7 Gestion des privilèges

a) L'entrepreneur doit gérer et surveiller les accès privilégiés à la SNC pour s'assurer que les interfaces de service sont protégées contre les accès non autorisés. Ce processus doit, au minimum :

i) permettre le renforcement et la vérification des autorisations d'accès aux données de la SNC;

ii) restreindre et minimiser l'accès seulement aux appareils autorisés et aux utilisateurs et aux administrateurs ayant explicitement besoin de cet accès;

iii) restreindre tout l'accès aux interfaces de service qui hébergent des données de la SNC aux personnes ayant un identifiant, une authentification et une autorisation uniques;

iv) mettre en place des mécanismes d'authentification à facteurs multiples pour authentifier les utilisateurs ayant des privilèges d'accès;

v) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux données de la SNC;

vi) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, ainsi que les rôles de développement des rôles opérationnels, et les rôles de gestion de l'accès des autres rôles opérationnels;

vii) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux employés et aux entrepreneurs;

viii) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure;

ix) mettre en place un processus automatisé ou manuel pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum – si un processus manuel de vérification est utilisé, la politique ou la procédure connexe doit être documentée et transmise au Canada;

x) révoquer, en cas de cessation d'emploi ou de contrat, les authentifiants et les justificatifs d'accès associés à l'employé ou au sous-traitant.

5.4.8 migration et échange de données sécurisés

a) L'entrepreneur doit appliquer les pratiques de migration de données ci-dessous pour soutenir la mise en œuvre de la SNC :

i) Entre l'entrepreneur et ses sous-traitants

L'entrepreneur doit utiliser la solution de transfert sécurisé de fichiers (MSFT) approuvée par le gouvernement du Canada pour la migration et l'échange sécurisé de données entre lui-même et ses sous-traitants (le cas échéant), qui prend en charge le protocole Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol over Secure Socket Layer (FTPS) et File Transfer Protocol over Secure Shell (SFTP) et comprend un système de cryptographie conforme à la norme Federal Information Processing Standard (FIPS 140-2).

ii) Entre l'entrepreneur et le Canada

L'entrepreneur doit établir des connexions réseau sécurisées appliquant le protocole TLS 1.2 ou une version subséquente, qui utilisent les algorithmes cryptographiques et les certificats approuvés par le Centre de la sécurité des télécommunications :

• Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) du CST, section 3.1 sur les suites de chiffrement TLS;

• Algorithmes cryptographiques pour l'information non classifiée, protégé A et protégée B (ITSP.40.111) du CST.

L'entrepreneur doit tenir à jour ses connexions réseau sécurisées conformément aux exigences du CST, qui pourraient évoluer au cours du contrat.

iii) Entre l'entrepreneur et un tiers

Après avoir obtenu l'approbation de l'autorité responsable du projet et de la Division de filtrage de la sécurité du personnel (anciennement la DSIC), l'entrepreneur doit fournir un outil ou une méthode de transfert de données sécurisé lui permettant de transférer des données à un tiers approuvé afin de faciliter les vérifications externes et d'autres projets lancés par le gouvernement.

5.4.9 Protection cryptographique

a) L'entrepreneur doit utiliser des mesures de protection cryptographique et les mettre à jour, si cela est jugé nécessaire après discussion avec le Canada, afin d'assurer la protection des données personnelles ou des mesures de protection de l'intégrité dans le cadre du mécanisme d'authentification (p. ex. solutions VPN, TLS, modules logiciels, ICP, jetons d'authentification, le cas échéant) utilisé pour le service.

b) L'entrepreneur doit utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des cryptopériodes approuvés, ce qui comprend :

i) des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été approuvés par le Centre de la sécurité des télécommunications et validés par le Programme de validation des algorithmes cryptographiques du NIST et qui sont précisés dans le document ITSB-111 ou dans une version ultérieure;

ii) une mise en œuvre et une utilisation dans un mode approuvé d'un module cryptographique validé par le Programme de validation des modules

cryptographiques du NIST et qui répond au moins aux exigences du NIST en matière de sécurité des modules cryptographiques (FIPS 140-2) de niveau 1. Au minimum, une cryptographie conforme à la norme FIPS 140-2 et validée doit être utilisée pour les dispositifs de protection du périmètre et partout où le chiffrement est requis.

5.4.10 Sécurité de l'échange de données informatisées

a) L'entrepreneur doit s'assurer que les données de la SNC fournies ou échangées entre le GNCC et des partenaires au moyen de l'EDI ou d'autres services numériques répondent à toutes les exigences en matière de sécurité de la SNC.

b) La solution de l'entrepreneur doit permettre la transmission sécurisée de renseignements par EDI entre les partenaires et le GNCC.

c) La solution de l'entrepreneur doit protéger l'intégrité et l'authenticité de l'ensemble des données de la SNC, qu'elles soient entreposées ou en mouvement. Elle doit aussi protéger les données contre la corruption et les modifications accidentelles ou malveillantes au moyen de hachage, de certificats numériques ou de technologies similaires, conformément à la norme 5.4.10 sur la protection cryptographique.

d) L'entrepreneur doit s'assurer que la sécurité et la protection de l'information sont maintenues au moment de la conversion ou du téléchargement de données.

5.4.11 Stockage et conservation des données

a) L'entrepreneur doit conserver toutes les données de récupération de la SNC conformément aux exigences du GNCC en matière de conservation de l'information et aux suivantes :

i) toute manipulation de supports de stockage de données portatifs pouvant être utilisés avec le système doit être conforme aux exigences en matière d'étiquetage, de destruction, de manipulation et d'entreposage de ces biens énoncées dans l'avis Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada (AMPTI 2014-01) ;

ii) toutes les données de récupération doivent être conservées à un endroit sûr et à l'abri des incendies et des inondations;

iii) les mesures de protection et de conservation des données doivent satisfaire à la norme Advanced Encryption Standard (AES), avec des longueurs de clé de 128 bits, afin d'assurer la protection et l'intégrité des données de récupération au lieu de stockage;

iv) l'entrepreneur doit vérifier s'il est possible de réutiliser en toute sécurité un dispositif de stockage, selon les lignes directrices du CST sur le nettoyage des supports de TI (ITSP.40.006) ;

v) l'entrepreneur est responsable des coûts associés à toute destruction de données amorcée par lui et approuvée par l'autorité responsable du projet.

5.4.12 Extraction de données

a) L'entrepreneur doit fournir les outils et les services nécessaires pour que le Canada puisse :

i) extraire toutes les données en ligne, pseudo-directes et hors ligne du Canada, y compris, au minimum, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes source hébergés dans un référentiel de codes du Canada et les configurations réseau, de sorte que tout utilisateur final du Canada puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;

ii) effectuer le transfert sécurisé de toutes les données du Canada, y compris les données de contenu et les métadonnées connexes, dans un format lisible et utilisable par machine (y compris le format CSV) et conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada .

5.4.13 Destruction des données

a) À la fin de la période du contrat (c.-à-d. à l'expiration ou à la résiliation du contrat) ou à la demande de l'autorité responsable du projet, l'entrepreneur doit suivre les lignes directrices du CST sur le nettoyage des supports de TI (ITSP.40.006) contenant des données de la SNC.

b) L'entrepreneur doit prouver à l'aide de pièces justificatives, comme un certificat, que toutes les données d'utilisateur associées à la SNC ont été détruites.

c) L'entrepreneur est responsable de tous les coûts liés à la destruction de supports ayant contenu de l'information protégé B de la SNC.

5.4.14 Transport des données

a) Si des données en format papier doivent être transportées physiquement, l'entrepreneur doit respecter le guide de la GRC G1-009 – Transport et transmission de renseignements protégés ou classifiés et le Manuel de la sécurité des contrats – Chapitre 6 : Manipulation et protection de renseignements et de biens.

b) L'entrepreneur doit marquer tous les documents en format papier et les autres supports de la classification de sécurité appropriée la plus élevée, selon l'autorité responsable du projet.

c) L'entrepreneur doit obtenir l'approbation de l'autorité responsable du projet avant d'entrer ou de sortir des données de leur emplacement physique protégé B.

5.5 Accès utilisateur autorisé

5.5.1 Attestation de sécurité du personnel

a) L'entrepreneur doit s'assurer que toutes les personnes qui traitent, consultent, gèrent ou sont en contact avec des données de la SNC ou qui ont accès aux installations

de la SNC ont une attestation de sécurité valide, soit une cote de fiabilité ou un niveau de sécurité supérieur, selon les exigences du gouvernement du Canada en matière de niveaux de sécurité. L'entrepreneur doit également s'assurer que les nouveaux membres du personnel, y compris les sous-traitants, possèdent les attestations appropriées et qu'ils les conservent tout au long du contrat.

b) L'entrepreneur doit s'assurer que les mesures de vérification du personnel sont appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du gouvernement du Canada afin de protéger adéquatement les renseignements protégé B.

5.5.2 Contrôles d'accès

a) L'entrepreneur doit prévoir des mesures de contrôle d'accès basé sur les rôles comme suit :

i) l'entrepreneur doit intégrer des contrôles d'accès basés sur les rôles définis dans la SNC – chaque rôle se voit attribuer des capacités et un accès en fonction du droit d'accès minimal requis pour ce rôle et du besoin de savoir;

ii) l'entrepreneur doit mettre en œuvre un processus pour gérer les comptes uniques de tous les utilisateurs de la SNC autorisés par l'autorité responsable du projet, de ses données protégé B ou, à tout le moins, des interfaces du P3 et de la SNC;

iii) l'entrepreneur doit apporter aux profils d'accès utilisateur les changements demandés dans les trois jours suivant la réception de la demande de l'autorité responsable du projet.

b) L'entrepreneur doit mettre en œuvre des mécanismes d'authentification à facteurs multiples pour les utilisateurs et les comptes privilégiés.

c) L'entrepreneur doit s'assurer que les mots de passe répondent aux exigences du Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031) du CST.

d) La page de confirmation de la connexion de la SNC doit indiquer la date et l'heure de la dernière connexion réussie.

e) Tout changement apporté à un compte utilisateur doit être accompagné d'un document de contrôle indiquant la nature du changement, le compte utilisateur à l'origine du changement, ainsi que la date, l'heure et l'auteur du changement.

f) L'entrepreneur doit tenir à jour ses contrôles et accès utilisateurs, selon les changements au sein du personnel, et aviser l'autorité responsable du projet de tout changement à cet égard.

5.5.3 Protection des comptes

a) L'entrepreneur doit appliquer des contrôles pour la génération de mots de passe et la mise à jour des mots de passe existants qui s'harmonisent l'un ou l'autre des éléments suivants :

i) le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031) du CST;

ii) d'autres pratiques exemplaires de l'industrie, comme la norme ISO 27001 ou celles du NIST.

5.5.4 Sensibilisation à la sécurité et formation

a) L'entrepreneur doit fournir une formation de sensibilisation à la sécurité ou une séance d'information afin que tous les membres du personnel (y compris les sous-traitants) qui traitent des renseignements protégé B de la SNC comprennent leur rôle et leurs responsabilités quant à la gestion de la sécurité de l'information avant de commencer à utiliser la SNC.

5.6 Essai des mécanismes de sécurité

a) L'entrepreneur doit présenter au Canada un plan d'essai des mécanismes de sécurité qui documente les jeux d'essai destinés à vérifier chaque exigence d'assurance de la sécurité de l'environnement de production de la SNC (EP de la SNC), marqué aux fins d'essai des mécanismes de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité.

b) L'entrepreneur doit exécuter le plan d'essai des mécanismes de sécurité à l'égard de chaque mesure de sécurité et présenter au gouvernement du Canada un rapport sur les essais des mécanismes de sécurité qui satisfait à une ou plusieurs des exigences de sécurité marquées aux fins d'essai des mécanismes de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité.

i) les procédures d'essai doivent confirmer que les mécanismes de sécurité sont mis en œuvre correctement et qu'ils respectent les normes applicables précisées dans les spécifications de la conception du service;

ii) les résultats prévus et ceux obtenus pour chaque procédure d'essai des mécanismes de sécurité;

iii) une description des mesures correctives apportées à l'EP de la SNC pour chacun des écarts constatés par rapport aux résultats prévus ayant pu être corrigés au moment de la vérification;

iv) un renvoi à une demande de modification de chacun des écarts par rapport aux résultats prévus n'ayant pu être corrigés au moment de la vérification (p. ex. parce que la correction aurait entraîné des modifications plus importantes).

c) L'entrepreneur doit mettre à jour la MTES afin d'inclure le suivi entre les exigences de sécurité marquées aux fins d'essai des mécanismes de sécurité et les procédures d'essai.

d) L'entrepreneur doit permettre au gouvernement du Canada d'assister à l'essai des mécanismes de sécurité, ce qui comprend la possibilité d'observer les représentants de l'entrepreneur pendant qu'ils exécutent les procédures d'essai des mécanismes de sécurité ou la capacité de consulter les résultats du journal d'essai lorsque l'essai des mécanismes de sécurité est automatisé.

5.7 Méthodes d'évaluation des contrôles de sécurité

a) L'entrepreneur doit utiliser les méthodes d'évaluation des contrôles de sécurité suivantes dans le rapport d'essai et d'évaluation des mécanismes de sécurité :

i) MÉTHODE D'ÉVALUATION : Examen :

(1) OBJETS VISÉS PAR L'ÉVALUATION :

a) Spécifications (p. ex. politiques, plans, procédures, exigences du système, conceptions);

b) Mécanismes (p. ex. fonctionnalité mise en œuvre dans le matériel, logiciel, micrologiciel);

c) Activités (p. ex. opérations, administration, gestion du système; exercices).

(2) DÉFINITION : La vérification, l'inspection, la revue, l'observation, l'étude ou l'analyse d'un ou de plusieurs objets pour faciliter la compréhension, apporter des éclaircissements ou obtenir des données probantes; les résultats contribuent à déterminer l'existence, la fonctionnalité, l'exactitude, l'exhaustivité et la possibilité d'amélioration des contrôles de sécurité au fil du temps;

ii) MÉTHODE D'ÉVALUATION : Essai :

(1) OBJETS VISÉS PAR L'ÉVALUATION :

a) Mécanismes (p. ex. matériel, logiciel, micrologiciel);

b) Activités (p. ex. opérations, administration, gestion du système; exercices).

(2) DÉFINITION : La mise à l'essai d'un ou de plusieurs objets dans des conditions précises pour comparer le rendement réel avec le rendement souhaité; les résultats contribuent à déterminer l'existence, la fonctionnalité, l'exactitude, l'exhaustivité et la possibilité d'amélioration des contrôles de sécurité au fil du temps.

5.8 Évaluation des vulnérabilités

a) L'entrepreneur doit permettre que les essais d'évaluation des vulnérabilités internes soient réalisés au fur et à mesure des besoins par le gouvernement du Canada, l'entrepreneur ou un tiers choisi par le gouvernement du Canada ou par l'entrepreneur. Ces essais d'évaluation doivent être réalisés au minimum chaque année et alignés sur les contrôles de gestion des vulnérabilités dans le PCMS. L'entrepreneur doit déterminer l'attribution de la responsabilité liée au soutien des essais d'évaluation des vulnérabilités.

b) Si l'entrepreneur choisit de permettre au Canada de réaliser les essais d'évaluation des vulnérabilités internes, l'entrepreneur doit fournir :

i) l'accès logique à l'espace infonuagique Protégé B de la GRC où l'infrastructure de l'environnement d'essai de la SNC (EE de la SNC) est située et exploitée;

ii) l'accès réseau (ou les accès, s'il y a lieu) à l'EE de la SNC afin de permettre l'analyse du réseau et des périphériques hôtes;

iii) l'aide d'au moins un (1) membre du personnel technique qui connaît bien les aspects techniques de l'infrastructure de l'EE de la SNC (c.-à-d. le matériel et les produits du réseau, ainsi que leur configuration) pendant la partie des essais d'évaluation des vulnérabilités internes réalisés.

c) Si l'entrepreneur (ou un tiers agissant au nom de l'entrepreneur) décide de mener ses propres essais d'évaluation des vulnérabilités internes, il doit :

i) soumettre un plan d'évaluation des vulnérabilités au gouvernement du Canada pour approbation préalable;

ii) inclure dans la portée du plan l'analyse de l'ensemble du réseau et des périphériques hôtes déployés dans l'EE de la SNC;

iii) réaliser les essais d'évaluation des vulnérabilités dans l'EE de la SNC;

iv) fournir les résultats au gouvernement du Canada pour examen et analyse. Le gouvernement du Canada peut exiger la mise en œuvre des changements initiés par l'entrepreneur en fonction d'un examen et d'une analyse.

d) Le gouvernement du Canada peut réaliser des essais d'évaluation des vulnérabilités externes par rapport à l'EE de la SNC et fournir à l'entrepreneur un rapport d'évaluation des vulnérabilités qui indiquera les vulnérabilités détectées par le gouvernement du Canada.

e) L'entrepreneur doit présenter au gouvernement du Canada un rapport sur l'atténuation des vulnérabilités qui comprend :

i) une liste de vulnérabilités pour lesquelles le gouvernement du Canada recommande la mise en œuvre de mesures correctives;

ii) une liste des vulnérabilités pour lesquelles l'entrepreneur recommande la mise en œuvre de mesures correctives s'il a choisi de mener ses propres essais d'évaluation des vulnérabilités internes;

iii) une description des mesures correctives à mettre en œuvre qui comprend les délais prévus;

iv) les documents sur les services mentionnés dans la MTES qui doivent être mis à jour en raison de la mise en œuvre de mesures correctives.

f) L'entrepreneur doit mettre en œuvre les mesures correctives indiquées dans le rapport d'atténuation des vulnérabilités approuvé dans le délai qui y est établi.

3.0 La section 4.0, paragraphe a) iii, Appendice B à l'Annexe C Obligations en matière de sécurité est SUPPRIMÉE et REMPLACÉE par:

« 4.0 Disposition des dossiers et remise des dossiers au Canada.

a) L'entrepreneur doit, à la demande du Canada, éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des actifs d'information et s'assurer que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela touche toutes les copies des actifs d'information du Canada qui sont créées à des fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'un des documents suivants : (i) Manuel d'utilisation du Programme national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et déclassification des supports d'information électroniques (CSTC ITSG-06).

L'ITSP.40.006 v2 Nettoyage des supports de TI est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).
Il remplace l'ITSG-06 Effacement et déclassification des supports d'information électroniques.
https://cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006

4.0) **Questions et réponses;**

Numero	**Question**	Réponse
1	**Section 1.2 Résumé** Cette section décrit le processus d'approvisionnement agile en plusieurs phases. Le Canada peut-il préciser dans quel délai il prévoit que toutes les étapes décrites à la section 1.2 j) seront terminées?	Réponse 1 Les phases du processus d'approvisionnement agile décrites illustrent les attentes du Canada pour la mise en œuvre de la solution complète. Les délais de livraison de chaque phase dépendront de plusieurs considérations, y compris des délais indiqués dans le document de demande de soumissions.
2	**3.1 Instructions pour la préparation des soumissions** Cette section indique que « Le soumissionnaire doit présenter les	Les soumissionnaires doivent fournir chacune des sections de la soumission demandées dans un fichier PDF, conformément aux instructions pour la préparation de la soumission.

	sections suivantes de sa soumission dans un (1) fichier PDF ». Veuillez confirmer que chaque section de la réponse du soumissionnaire (Soumission technique, Soumission financière, Attestations, etc.) doit être présentée dans un document PDF distinct.	
3	**3.4 Section I : Soumission technique** Cette section décrit ce qui doit être fourni dans la Soumission technique, y compris le formulaire de présentation de soumission, la documentation technique, les références, etc. Elle n'indique pas explicitement que les soumissionnaires doivent fournir une réponse détaillée à l'Annexe J dans la soumission technique. Veuillez confirmer si les soumissionnaires doivent répondre à l'Annexe J dans la soumission technique et, le cas échéant, modifier la section 3.4 en conséquence. Cette section indique aussi que les soumissionnaires doivent fournir une liste de logiciels proposés qui feront partie de la solution, au point (v). Veuillez apporter des précisions, car au point 3,6 Section III : Attestations, on demande aussi aux soumissionnaires de fournir l'Information sur la sécurité de la chaîne d'approvisionnement (ISCA). Est-ce que la liste de logiciels doit être fournie dans la Soumission technique et dans l'ISCA qui est requise à la section Attestations? De plus, est-ce que le Canada fournira aux soumissionnaires un fichier Excel de l'ISCA et est-ce que l'ISCA est requise avec la présentation de soumission ou à une étape ultérieure du processus d'approvisionnement agile en plusieurs phases, quand la version définitive de la solution aura été établie?	Les soumissionnaires doivent faire référence au document de demande de soumissions dans son intégralité, y compris les parties 3, 4 et 5 collectivement. La soumission technique des soumissionnaires doit répondre aux critères de l'Annexe J – Critères d'évaluation technique et à toute autre exigence de la demande de propositions (DP). Les soumissionnaires doivent satisfaire aux exigences en matière d'attestation dans la section sur les attestations de leur soumission, conformément au document de demande de soumissions. Les soumissionnaires doivent fournir l'information sur l'intégrité de la chaîne d'approvisionnement (ICA) dans la section sur les attestations de leur soumission, conformément à la partie 5 de la DP et au processus d'ICA indiqué dans la DP.

4	Nous ne sommes pas en mesure d'identifier efficacement les changements apportés par le Canada dans la modification 1. Nous demandons respectueusement au Canada de fournir aux soumissionnaires une liste complète des changements apportés par section et de confirmer que les changements futurs seront communiqués de la manière traditionnelle, c'est-à-dire par section modifiée « de – à ».	La modification 1 publiée indique expressément que le nouveau document de demande de soumissions remplace dans son intégralité le document de demande de soumissions publié précédemment. Le document de demande de soumissions en entier est maintenant remplacé par le document publié, conformément à la modification 1. Étant donné que le Canada a remplacé un document dans son intégralité, il ne fournira pas une liste exhaustive des changements. Si des modifications ultérieures sont apportées à une section du document de demande de soumissions, elles seront communiquées en informant les soumissionnaires de la ou des sections modifiées et en indiquant que toutes les autres sections du document demeurent inchangées.
5	**Section 2.1 Instructions, clauses et conditions uniformisées** Cette section incorpore par renvoi les modalités des Instructions uniformisées 2003 (2020-05-28) du Guide des clauses et conditions uniformisées d'achat (CCUA), incluant la clause « Définition de soumissionnaire » de la section 04, qui exclut la société mère, les filiales ou autres sociétés affiliées du soumissionnaire ou de ses sous-traitants. Compte tenu de la nature unique de la présente demande de propositions, qui traite des services de police et de la cybersécurité, il est dans l'intérêt du Canada de pouvoir compter sur des soumissionnaires qualifiés qui possèdent une expérience mondiale dans le domaine des services policiers et des solutions en matière de sécurité. En raison de notre structure d'entreprise, de tels travaux dans d'autres lieux géographiques sont effectués par notre société mère aux États-Unis ou nos sociétés affiliées dans d'autres pays. Veuillez confirmer que nous pouvons nous servir de l'expérience mondiale de	Les soumissionnaires doivent se reporter à la demande de propositions, partie 3, article 3.4, section I : Soumission technique, section (b) (iii); « (iii) Projets antérieurs semblables : Si la soumission doit comprendre la description de projets antérieurs semblables : i) le projet doit avoir été réalisé par le soumissionnaire lui-même (l'expérience acquise par un sous-traitant proposé ou une société affiliée au soumissionnaire ne compte pas); ii) toutes les descriptions de projet doivent comprendre, au minimum, le nom et le numéro de téléphone ou l'adresse de courriel d'un client cité en référence; et iii) si le soumissionnaire présente plus de projets semblables que ce qui a été demandé, le Canada aura le plein pouvoir de choisir ceux qui seront évalués. Un projet sera jugé « similaire » aux travaux à effectuer dans le cadre du contrat subséquent s'il porte sur des travaux qui correspondent étroitement aux descriptions indiquées à l'annexe A, Énoncé des travaux. Les travaux seront considérés comme « correspondant étroitement » si la description du projet inclut au moins 50 % des points de

	notre société mère ou de nos sociétés affiliées pour satisfaire aux exigences relatives aux références d'entreprises, et modifier la disposition 3.4 b) iii) en conséquence.	responsabilité figurant dans la description de la catégorie de ressources donnée.
6	Tous les membres d'une coentreprise devront-ils avoir une attestation de sécurité pour l'installation au moment de la clôture des soumissions?	Tous les membres d'une coentreprise devront détenir une ASI avant que le contrat soit attribué.
7	Tous les membres d'une coentreprise devront-ils détenir une autorisation de détenir des renseignements avant la clôture des soumissions?	Tous les membres d'une coentreprise qui recevront ou conserveront des renseignements ou des biens protégés ou classifiés dans leurs installations devront détenir une ADR avant que le contrat soit attribué.
8	En vue de la présentation de soumissions dans le cadre de la présente demande ou de demandes similaires, accepteriez-vous de parrainer une entreprise pour l'obtention d'une ASI et d'une ADR?	Oui, les organisations qui désirent être parrainées doivent communiquer les informations organisationnelles requises en remplissant les sections A à D du formulaire ci-joint et transmettre ce formulaire à l'autorité contractante.  186.pdf
9	Le Canada a reçu plusieurs demandes de prolongation de la soumission.	La date de fermeture de proposition est prolongée au 22 juin 2021.

TOUTES LES AUTRES MODALITÉS DE LA DEMANDE DE PROPOSITIONS DEMEURENT INCHANGÉES.

Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Contract Security Program
Programme de sécurité des contrats

Request for Private Sector Organization Screening (PSOS)
Demande d'enquête de sécurité sur une Organisation du Secteur Privé (ESOSP)

A **Type of application (check one)**
Type de demande (cocher une seule case)

☐ New / Nouvelle ☐ Upgrade / Cote de sécurité plus élevée

B **Information on proposed organization**
Renseignements sur l'organisation candidate

1 Legal name / Raison sociale	2 Business name (if different from legal name) / Nom de l'organisation (si différent de la raison sociale)
3 Mailing address - Adresse postale	4 Civic address - Adresse municipale
5 Organization telephone No.- N° de téléphone de l'organisation	6 Organization Fax No. - N° de télécopieur de l'organisation
7 Surname and given name of contact person (Canadian Official) / Nom et prénom de la personne-ressource au Canada	8 Title of contact person / Titre de la personne-ressource
9 Telephone No. of contact person / N° de téléphone de la personne-ressource	10 E-mail address of contact person / Adresse électronique de la personne-ressource

11 Preferred language of correspondence (check one) / Langue de correspondance (cocher une seule case) ☐ English / Anglais ☐ French / Français

C **Information on registered or head office in Canada (if different from section B)**
Renseignements sur le siège social ou le bureau principal au Canada (si différents de ceux fournis à la section B)

1 Legal name / Raison sociale	2 Business name (if different from legal name) / Nom de l'organisation (si différent de la raison sociale)
3 Civic address - Adresse municipale	

D **Reason(s) for PSOS request (check those that apply and provide details in space provided)**
Raison(s) de la demande d'ESOSP (cocher la ou les cases appropriées et fournir des détails dans l'espace prévu à cette fin)

☐ Contract or RFP (provide number) / Contrat ou DDP (indiquer le numéro) ▸ _____

☐ Sub-contract (provide number) / Contrat accordé en sous-traitance (indiquer le numéro) ▸ _____

☐ Program or project (provide name) / Programme ou projet (indiquer le nom) ▸ _____

☐ Major Crown project (provide name) / Grand projet de la Couronne (indiquer le nom) ▸ _____

☐ Other (provide details) / Autres (donner des détails) ▸ _____

E **Information on security requirements**
Renseignements sur les exigences relatives à la sécurité

1- Indicate level(s) of personnel security screening required (check those that apply)
Indiquer le ou les niveaux requis de l'enquête de sécurité sur le personnel (cocher la ou les cases appropriées)

☐ Reliability status* / Cote de fiabilité*
☐ Secret
☐ NATO Secret / Secret OTAN
☐ Top Secret / Très secret
☐ COSMIC Top Secret / COSMIC Très secret

* This level is required for access to Protected A, Protected B and Protected C information or assets.
* Ce niveau est nécessaire pour l'accès à des renseignements ou à des biens Protégé A, B ou C.

Canada

E ▸ Information on security requirements (continued)
Renseignements sur les exigences relatives à la sécurité (suite)

2- Will the proposed organization be required to store protected/classified information/assets?
L'organisation candidate devra-t-elle entreposer des renseignements ou des biens de niveau protégé ou classifié?

☐ Yes / Oui ☐ No / Non

a) If yes, indicate security level(s) of information/assets to be stored (check those that apply).*
Also, provide address(es) where information/assets will be stored in section B and C below.
Si oui, indiquer le niveau de sécurité des biens ou des renseignements qui seront entreposés (cocher la ou les cases appropriées).*
Indiquer également, aux sections B et C ci-dessous, la ou les adresses où les renseignements/les biens seront entreposés.

☐ Protected A / Protégé A ☐ Protected B / Protégé B ☐ Protected C / Protégé C ☐ Confidential / Confidentiel ☐ NATO Confidential / Confidentiel OTAN

☐ Secret ☐ Top Secret / Très secret ☐ NATO Secret / Secret OTAN ☐ COSMIC Top Secret / COSMIC Très secret

* Please attach a completed Security Requirements Check List - Veuillez joindre la Liste de vérification des exigences relatives à la sécurité dûment remplie.

b) Civic address - Adresse municipale	c) Civic address - Adresse municipale

3- Will the proposed organization be required to store Protected/Classified COMSEC information/assets?
L'organisation candidate devra-t-elle entreposer des renseignements ou des biens relatifs à la sécurité des communications (COMSEC) Protégé ou Classifié?

☐ Yes / Oui ☐ No / Non

a) If yes, indicate security level(s) of Protected/Classified COMSEC information/assets to be stored (check those that apply).
Si oui, indiquer le ou les niveaux de sécurité des renseignements ou des biens COMSEC Protégé ou Classifié qui seront entreposés (cocher la ou les cases appropriées).

☐ Protected A / Protégé A ☐ Protected B / Protégé B ☐ Protected C / Protégé C ☐ Confidential / Confidentiel ☐ Secret ☐ Top Secret / Très secret

4- Additional information - Renseignements additionnels

F ▸ Information on procurement Officer / project manager requesting PSOS (if different from section G)
Renseignements sur l'agent des achats ou le gestionnaire de projets qui demande l'ESOSP (si différents de ceux fournis à la section G)

1 Surname, Given name / Nom et prénom	2 Title/Rank / Titre et niveau hiérarchique
3 Department/Agency/Organization / Ministère, agence ou organisation	4 Branch/Directorate / Division/Direction
5 Mailing address - Adresse postale	6 E-mail address - Adresse électronique
	7 Telephone No. - N° de téléphone
	8 Facsimile No. - N° de télécopieur
9 Signature of procurement officer or project manager / Signature de l'agent des achats ou du gestionnaire de projet	Date (Y-A-MM-D-J)

G ▸ Information on approved source requesting PSOS
Renseignements sur la source autorisée parrainant l'ESOSP

1 Surname, Given name / Nom et prénom	2 Title/Rank / Titre et niveau hiérarchique
3 Department/Agency/Organization / Ministère, agence ou organisation	4 Branch/Directorate / Division/Direction
5 Mailing address - Adresse postale	6 E-mail address - Adresse électronique
	7 Telephone No. - N° de téléphone
	8 Facsimile No. - N° de télécopieur
9 Signature of approved source / Signature de la source autorisée	Date (Y-A-MM-D-J)