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.** 003
Client Reference No. - N° de référence du client M7594-205915	**Date** 2021-05-10
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 003 de l'ìnvitation à:

1. Modifier la section 3.20, énoncé de travaux; paragraphe a) Annexe A
2. Modifier la section 5.0, énoncé de travaux; paragraphe 5.8 Annexe A
3. Soumissionner vise à publier les questions et réponses.

1. La section 3.20 énonce de travaux; paragraphe a) - Annexe A est SUPPRIMÉE et REMPLACÉE par:

3.20 **Règles pour l'accessibilité des contenus Web (WCAG)**

a) La solution doit être conforme aux WCAG 2.0 niveau A et à la norme sur l'accessibilité du Web du gouvernement du Canada, comme suit :

i) La solution doit être accessible à l'aide de technologies d'assistance et de divers navigateurs Web, tels qu'Internet Explorer, Firefox, Chrome, Safari et Edge.

ii) L'information, la structure et les relations véhiculées par la présentation doivent être déterminées par un programme informatique ou sont disponibles sous forme de texte.

iii) Lorsque l'ordre de présentation du contenu a un effet sur sa signification, un ordre de lecture correct doit être déterminé par programme informatique.

iv) Toutes les fonctions du contenu doivent être contrôlées par une interface clavier qui n'exige pas de rythmes de frappe particuliers, sauf lorsque la fonction sous-jacente nécessite des données indiquant la trajectoire donnée par l'utilisateur en plus des points finaux.

v) Si la cible de saisie du clavier peut être positionnée sur un élément de la page à l'aide d'une interface clavier, réciproquement, elle peut être déplacée hors de cette même composante simplement à l'aide d'une interface clavier et, si ce déplacement exige plus que l'utilisation d'une simple touche flèche ou tabulation ou toute autre méthode standard de sortie, l'utilisateur est informé de la méthode permettant de déplacer la cible de saisie hors de cette composante.

vi) Un mécanisme doit permettre de contourner les blocs de contenu reproduits dans plusieurs pages Web.

vii) Quand une composante de l'interface utilisateur reçoit la cible de saisie, il ne doit pas amorcer un changement de contexte.

viii) Le changement de paramètre d'une composante d'interface utilisateur ne doit pas entraîner de changement de contexte, à moins que l'utilisateur n'ait été avisé de ce comportement avant d'utiliser la composante.

ix) À moins que les spécifications ne le permettent, dans un contenu mis en œuvre au moyen d'un langage de balisage, les éléments ont des balises de début et de fin complètes, ils sont imbriqués conformément à leurs spécifications, ils ne doivent pas contenir d'attributs dupliqués, et chaque ID doit être unique.

x) Pour toute composante d'interface utilisateur (comprenant, mais sans y être limité, des éléments de formulaire, liens et composantes générés par des scripts), le nom et le rôle doivent être déterminés par un programme informatique; les états, les propriétés et les valeurs qui peuvent être paramétrés par l'utilisateur doivent être définis par programmation, et la notification des changements de ces éléments doit être accessible aux agents utilisateurs, y compris les technologies d'assistance.

xi) Le contenu ne doit pas limiter son affichage et son fonctionnement à une seule orientation d'affichage, comme le portrait ou le paysage, à moins qu'une orientation d'affichage spécifique soit essentielle.

xii) Dans un ensemble de pages Web, les mécanismes de navigation qui se répètent sur plusieurs pages Web doivent se présenter dans le même ordre relatif chaque fois qu'ils sont répétés, à moins qu'un changement soit amorcé par l'utilisateur.

xiii) Dans un ensemble de pages Web, les composantes qui ont la même fonction doivent être identifiées de la même façon.

xiv) Toute interface utilisateur utilisable au clavier doit avoir un mode de fonctionnement dans lequel l'indicateur de mise au point du clavier est visible.

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 .

b) 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 .

c) 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).

b) 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.

c) 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 est chargé des essais d'évaluation des vulnérabilités internes et externes, qui doivent être réalisés par l'entrepreneur ou un tiers approuvé par le Canada, au fur et à mesure des besoins. Ces essais d'évaluation doivent être effectués au minimum chaque année et alignés sur les contrôles de gestion des vulnérabilités dans le PCSM. L'entrepreneur doit déterminer l'attribution de la responsabilité liée au soutien des essais d'évaluation des vulnérabilités.

b) L'entrepreneur doit prendre des dispositions pour permettre au Canada, ou à un tiers agissant au nom du Canada, d'effectuer des essais d'évaluation de la vulnérabilité interne et externe, selon les besoins.

c) Lorsque le Canada demande que le Canada, ou un tiers agissant au nom du Canada, effectue les essais d'évaluation de la vulnérabilité, 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. les produits logiciels et les produits réseau ainsi que leur configuration) pendant la partie des essais d'évaluation des vulnérabilités internes réalisés.

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

i) soumettre un plan d'évaluation des vulnérabilités au 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 Canada pour examen et analyse. Le Canada peut exiger la mise en œuvre des changements initiés par l'entrepreneur en fonction d'un examen et d'une analyse.

e) En réponse à toute source de vulnérabilité détectée durant les essais d'évaluation, l'entrepreneur doit présenter au Canada dans les dix (10) jours ouvrables suivants 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 est établi dans ce rapport.

2.0 **Questions et réponses;**

GRC/SPAC Référence # Question	**Question**	**Réponse**
10	**La partie 7.8(c) de la demande de propositions qui porte sur les droits de traduction précise que :** « L'entrepreneur convient que le Canada peut traduire tout produit livrable écrit, y compris la documentation sur la solution ou les documents de formation, en anglais ou en français. » Cependant, la partie 3.10.2 Matériel de formation a) de l'énoncé des travaux stipule que « l'entrepreneur doit fournir des copies électroniques en anglais et en français des manuels d'utilisation, des manuels techniques et de tout autre document à l'intention de l'utilisateur requis pour lui permettre d'apprendre, d'utiliser et de tenir à jour la solution », etc. L'État peut-il préciser s'il est obligatoire que les manuels d'utilisation, les manuels techniques et tout le matériel de formation soient traduits par l'entrepreneur?	Le Canada exige que l'entrepreneur fournisse des copies électroniques en anglais et en français des manuels d'utilisation, des manuels techniques et de tout autre document requis à l'intention de l'utilisateur pour lui permettre d'apprendre, d'utiliser, et de tenir à jour la solution.

11	**La partie 3.4.b.ii de l'énoncé des travaux indique que l'EAS fait partie de la phase 2.** Le Canada peut-il confirmer que les processus d'EAS pour la phase 1 n'ont pas besoin d'être mis en œuvre et ne seront requis que si le Canada invoque son option d'entreprendre la phase 2?	Le processus d'EAS n'est requis qu'après que le Canada ait sélectionné un entrepreneur pour la phase 2.
12	**Le tableau 3-1 Paramètres de rendement de la partie 3.18 de l'énoncé des travaux précise les paramètres de temps de réaction maximal.** Le Canada a-t-il l'intention de mesurer à partir du navigateur ou à partir du moment où les paramètres quittent le point d'extrémité du réseau contrôlé par l'entrepreneur?	Le Canada entend mesurer les paramètres indiqués à partir du navigateur (interface de l'utilisateur final). Toutefois, l'entrepreneur ne sera pas tenu responsable des retards qui se produisent en dehors des points d'extrémité du réseau qu'il contrôle.
13	**La partie 3.20 Règles pour l'accessibilité des contenus Web 1.0 (WCAG) de l'énoncé des travaux fait référence aux WCAG 2.0, mais ne précise pas le niveau (A ou AA) qui doit être atteint.** Le point 5.13.2.2 de l'annexe C fait mention de la WCAG 2.0 A. Le critère obligatoire MC-47 de l'annexe J est en phase avec la partie 3.20 de l'énoncé des travaux. Le Canada peut-il confirmer que la WCAG 2.0 de niveau A est celle exigée?	Voir la modification de la section 3.20, énoncé de travaux; paragraphe a) Annexe A
14	**Les rubriques a. iv, v, vi, vii, xiv et xi de la partie 4.3 Interopérabilité de l'énoncé des travaux font référence à diverses interfaces.** Le Canada peut-il confirmer que toutes ces interfaces, qui sont basées sur des API, supportent le service REST, le protocole JSON ou le format XML?	Le Canada confirme que ces interfaces basées sur des API supportent des protocoles qui incluent entre autres le transfert d'état de représentation (REST) qui utilise la notation d'objet JavaScript (JSON) ou le langage de balisage extensible (XML).

15	**La partie 4.3.b.i de l'énoncé des travaux évoque le service de mise en file d'attente du site Web de signalement destiné au public.** Le Canada peut-il fournir des informations sur le service de mise en file d'attente du site Web de signalement destiné au public qui a été sélectionné? Ce service n'apparaît pas sur le diagramme d'architecture du Canada à l'annexe D.	Comme le décrit la partie 4.4 de l'énoncé des travaux, l'architecture et la conception d'une interface de mise en file d'attente des messages qui intègrent les rapports du site Web de signalement destiné au public du Canada dans la SNC devraient faire partie de la solution de l'entrepreneur. Aucune mise en œuvre n'existe actuellement pour le site Web de signalement destiné au public.
16	**Les parties 4.6.a, 3.12 et 3.14 de l'énoncé des travaux ne semblent pas être en phase avec la transition vers la solution complète par le Canada.** La partie 3.12 Plan de transition de l'énoncé des travaux suggère que le plan de transition vise une transition complète au Canada en supposant le recours à l'espace infonuagique protégé B de la GRC. La partie 4.6.a évoque trois options qui incluent l'espace infonuagique protégé B de la GRC. Le Canada peut-il préciser comment le plan de transition devra tenir compte des trois options présentées à la partie 4.6.a?	Le Canada exige un plan de transition qui correspond à l'architecture de la solution du soumissionnaire. La partie 4.6 Déploiement infonuagique de l'énoncé des travaux décrit les exigences du Canada en ce qui concerne l'architecture liée au modèle de prestation de services infonuagiques de la solution. Les exigences du plan de transition évoquées dans l'énoncé des travaux ne prévoient pas l'utilisation de l'espace infonuagique protégé B de la GRC si cela ne correspond pas à la solution du soumissionnaire (par exemple, si la solution est une solution sous forme de services SaaS ou une plateforme publique comme service PaaS).
17	**La partie 4.7.a.iv de l'énoncé des travaux précise que :** Le développement des mises à jour et des nouvelles fonctionnalités doit être effectué sur l'espace infonuagique protégé B de la GRC dans un environnement de développement. Comment cette exigence se concilie-t-elle avec la partie 4.6.a où trois options sont décrites?	La partie 4.7 Code source et développement ne s'applique pas aux composants SaaS ou PaaS publiques de la solution. Pour les composants de l'infrastructure en tant que service IaaS et de la plateforme PaaS privée d'une solution qui impliquent le développement de codes et une configuration sur mesure, le Canada exige que l'entrepreneur fournisse une équipe d'intégration qui travaillera en collaboration avec la GRC, tel que précisé à la partie 4.7.

18	**La partie 4.8 de l'énoncé des travaux exige l'utilisation d'Azure AD pour l'accès administratif.** Notez que la partie 4.6.d.iv de l'énoncé des travaux précise que seule la plateforme Azure AD doit être utilisée pour gérer les utilisateurs internes de la GRC et les utilisateurs externes des partenaires. Quelle partie est correcte?	La solution doit utiliser la fonctionnalité Azure AD (Active Directory) pour gérer l'identité et l'accès de tous les utilisateurs de la solution (y compris les accès administratifs).
19	**La partie 5.6. a de l'énoncé des travaux stipule que :** Le plan de test de la sécurité doit intégrer les exigences en matière d'assurance de la sécurité de l'annexe E auxquelles doit répondre le test de sécurité. La partie 5.7 de l'énoncé des travaux comprend de l'information sur la méthode d'évaluation relative aux contrôles de type « examen » ou « test ». La lecture de l'annexe E ne permet pas de savoir quels aspects de la sécurité doivent être soumis à un examen et lesquelles doivent être soumises à un test. Le Canada fournira-t-il une annexe E mise à jour qui met en évidence les aspects de la sécurité qui sont soumis à un examen?	La section 5.7 présente les méthodes acceptables pour les essais, mais l'entrepreneur aura la possibilité de déterminer la méthode d'essai qu'il juge la plus appropriée pour un contrôle donné, sous réserve d'un examen par le Canada au cours du processus d'évaluation et d'autorisation de sécurité. Par conséquent, le Canada ne fournira pas de mise à jour de l'annexe E, mais s'attendra plutôt à ce que le fournisseur détermine la méthode d'évaluation appropriée pour chaque exigence d'assurance de la sécurité dans le plan d'essai de sécurité qu'il remettra au Canada.
20	**Partie 5.8 Évaluation de la vulnérabilité de l'énoncé des travaux :** Cette partie indique qu'il s'agit d'un service facultatif, comme indiqué ci-dessous : La partie 5.8 b) indique ceci : « Si l'entrepreneur choisit de permettre au Canada de réaliser les essais	Voir la modification de la section 5.0, énoncé de travaux; paragraphe 5.8 Annexe A.

	d'évaluation des vulnérabilités internes, l'entrepreneur doit fournir : **»** et La partie 5.8 c) indique ceci : « 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 : » Les soumissionnaires peuvent donc choisir d'effectuer eux-mêmes l'évaluation ou demander au Canada de l'effectuer. Comment le Canada s'assurera-t-il que l'évaluation financière est juste et équitable entre les soumissionnaires qui ont choisi d'inclure ou d'exclure ces coûts?	
21	**La partie 7.1.d de l'énoncé des travaux stipule que :** La phase 2 commence à la date à laquelle le gouvernement du Canada exerce son option de demander à l'entrepreneur de fournir la solution complète (travaux de phase 2). Est-ce l'intention du Canada que la phase 2 : a. Suive la phase 1 immédiatement après, sans interruption de service entre la fin de la phase 1 et le début de la phase 2? b. Suive la fin de la phase 1, mais avec un intervalle de plusieurs semaines ou de plusieurs mois entre la fin de la phase 1 et le début de la phase 2?	Le Canada a l'intention de lancer la phase 2 immédiatement après l'achèvement de la phase 1.

	c. Chevauche l'échéancier de la phase 1? Dans l'affirmative, de combien de semaines ou de mois?	
22	**Annexe C – Modèle de capacité opérationnelle de la SNC de l'énoncé des travaux; la capacité 2.1.2.4 évoque des taux de change.** Le Canada donne-t-il accès à une API qui fournira ces taux de change à la SNC?	La solution de l'entrepreneur doit offrir une fonction de conversion des devises conformément aux exigences énoncées dans le modèle de capacité opérationnelle.
23	**La capacité 5.2.2.5 de l'annexe C précise que la solution doit intégrer MS Outlook.** La capacité 5.7.1.3 précise que la SNC doit s'intégrer au système organisationnel de courriel de la GRC. MS Outlook est-il le système de messagerie de l'entreprise et est-il absent du tableau 4.1 Composants obligatoires de la GRC?	MS Outlook est le système de messagerie électronique de la GRC.
24	**L'annexe J Critères obligatoires et cotés MC-55 précise que :** Des preuves doivent être fournies qui démontrent une intégration réussie entre son programme de sécurité des contrats (PSC) et le réseau du gouvernement du Canada au moyen de l'infrastructure ADNS. Le Canada peut-il confirmer qu'aux fins de la phase 1, cette intégration doit avoir eu lieu à la date de clôture des soumissions de la présente DP? Dans l'affirmative, veuillez fournir une liste des PSC qui répondent à cette exigence et	Le Canada confirme que l'intégration entre le PSC proposé et le réseau du GC utilisant l'infrastructure ADNS doit exister à la date de clôture des soumissions de la présente DP. Une liste des PSC qui répondent à ces exigences est disponible en communiquant avec le service de courtage infonuagique du GC.

	préciser quels soumissionnaires qui ont l'intention d'utiliser un autre nuage ne seront pas conformes.	
25	**Mise en correspondance des critères obligatoires et des critères cotés de l'annexe J et des capacités de l'annexe C :** Le Canada peut-il fournir une cartographie de la traçabilité des critères obligatoires et des critères cotés de l'annexe J par rapport aux capacités correspondantes de l'annexe C? Cette traçabilité est nécessaire pour documenter l'écart entre les capacités de la phase 1 et de la phase 2 à fournir après la phase 1 et pour garantir que tous les soumissionnaires évaluent la même solution.	Le Canada ne fournira pas de cartographie de traçabilité. Le Canada s'attend à ce que les soumissionnaires répondent aux exigences énoncées à l'annexe C. Tout écart entre les capacités de la phase 1 et celles de la phase 2 sera comblé au cours de la phase 2.

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