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
epost Connect / Postel
Refer to section 2.2 of this ITQ
Réferez-vous à la section 2.2 de cette ISQ

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet ISQ pour SGPN/Caméras Corporelles	
Solicitation No. - N° de l'invitation M7594-212120/F	**Date** 2021-05-28
Client Reference No. - N° de référence du client M7594-212120	**GETS Ref. No. - N° de réf. de SEAG** PW-$$XV-001-39525
File No. - N° de dossier 001xv.M7594-212120	**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: Cummings, Kent	**Buyer Id - Id de l'acheteur** 001xv
Telephone No. - N° de téléphone (613) 866-3745 ( )	**FAX No. - N° de FAX** ( ) -

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

La Gendarmerie royale du Canada
1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein – Voir ci-inclus	**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**

Issuing Office - Bureau de distribution

Technology-Enabled Business Transformation Team 5 → XV/Division de la transformation des activités axées sur la technologie équipe 5
Terrasses de la Chaudière 4th Floo
Terrasses de la Chaudière 4e étage
10 Wellington Street
10, rue Wellington
Gatineau
Québec
K1A 0S5

Canada

INVITATION À SE QUALIFIER (ISQ)

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La présente Invitation à se qualifier (ISQ) contient 6 parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des Répondants : renferme les instructions aux clauses et conditions relatives à l'étape de l'ISQ;

Partie 3 Instructions pour la préparation des réponses : donne aux Répondants les instructions pour préparer l'ISQ afin de répondre aux critères d'évaluation spécifiés;

Partie 4 Procédures d'évaluation et sélection des Répondants retenus : décrit la façon selon laquelle se déroulera l'évaluation des réponses, les critères d'évaluation auxquels on doit répondre ainsi que la méthode de sélection des Répondants retenus.

Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir; et

Partie 6 Clauses anticipées de soumissions et de contrats subséquents, contient des informations générales sur les conditions qui peuvent s'appliquer à toute sollicitation ultérieure et à tout contrat subséquent conclu en vertu de cette phase de l'ISQ.

1.2 Termes-clés

Dans le présent document, à moins que le contexte ne l'exige autrement:

- « ISQ » signifie Invitation à se qualifier
- « partie intéressée » désigne une/des entité(s) intéressée(s) à présenter une soumission en réponse à la présente ISQ;
- « Répondant » s'entend d'une partie intéressée qui a soumis une réponse à cette ISQ. Le terme ne comprend pas la société mère, les filiales ou autres affiliées de la partie intéressée, ni ses sous-traitants.
- « Répondant provisoirement qualifié » s'entend d'un Répondant qui a été évalué par le Canada comme satisfaisant aux critères d'évaluation de l'annexe B, aux exigences et aux conditions énoncées dans l'ISQ, mais qui n'a pas encore été évalué dans le cadre du processus préliminaire de l'intégrité de la chaîne d'approvisionnement et l'évaluation de la propriété, du contrôle et de l'influence de l'étranger;
- «Répondant qualifié» (RQ) désigne un Répondant provisoirement qualifié qui a été évalué comme conforme dans le cadre du processus préliminaire de l'intégrité de la chaîne d'approvisionnement et l'évaluation de la propriété, du contrôle et de l'influence de l'étranger;
- « DDP » désigne la demande de propositions
- « TPSGC » désigne Travaux publics et Services Gouvernementaux Canada
- « GRC » désigne Gendarmerie royale du Canada

1.3 Portée

1.3.1 Le Canada souhaite attribuer un marché à un ou à des entrepreneurs qui fourniront une solution offrant des caméras corporelles et un logiciel-service (SaaS) de système de gestion de preuves numériques (SGPN) comme un service entièrement géré. L'annexe A – Aperçu et description de haut niveau du besoin contient un aperçu et la portée de l'exigence

1.3.2 La présente invitation à se qualifier (ISQ) est la première phase du processus d'approvisionnement de Travaux publics et Services gouvernementaux Canada (TPSGC), au nom de la Gendarmerie royale du Canada (GRC), pour les services gérés du SGPN national et des caméras corporelles. L'ISQ n'est ni une demande de propositions, ni une demande de soumissions, ni un appel d'offres. Elle ne donnera pas lieu à l'attribution d'un contrat. Le Canada se réserve le droit de modifier, de changer ou d'interrompre, à sa seule discrétion, l'une ou l'ensemble des phases du processus d'approvisionnement en tout temps pendant le processus d'approvisionnement. Comme le Canada peut annuler la présente ISQ, il se peut que les processus d'approvisionnement subséquents décrits dans le présent document ne soient jamais entamés. Les Répondants peuvent se retirer du processus à tout moment. La présente ISQ n'empêche pas le Canada de recourir à une autre méthode d'approvisionnement.

1.3.3 Les parties intéressées sont invitées à se soumettre à une sélection préalable, conformément aux modalités de la présente ISQ, afin d'être retenues comme « Répondant provisoirement qualifié » et « Répondants qualifiés » pour les phases ultérieures du processus d'approvisionnement. Le Canada a l'intention de présélectionner les Répondants en fonction des critères obligatoires énumérés à l'annexe B – Critères d'évaluation obligatoires. Les Répondants qui satisfont à toutes les exigences obligatoires de l'ISQ à l'issue d'une évaluation officielle effectuée au cours du processus d'ISQ seront appelés ci-après « Répondant provisoirement qualifié».

1.4 Utilisateurs clients potentiels

La Gendarmerie royale du Canada (GRC) est le client initial et le responsable technique. L'autorité contractante peut ajouter d'autres clients, notamment tout ministère ou toute société d'État mentionnés dans la *Loi sur la gestion des finances publiques* (et ses modifications) et toute autre partie au nom de laquelle Travaux publics et Services gouvernementaux Canada peut être autorisé à agir en vertu de l'article 16 de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*. La possibilité qu'a le Canada de mettre le contrat à la disposition d'un client ou de l'ensemble des clients ne l'empêche pas de recourir à une autre méthode d'approvisionnement.

1.5 Aperçu du processus d'approvisionnement

1.5.1 Le processus d'approvisionnement pour les services gérés du système de gestion de preuves numériques (SGPN) national et des caméras corporelles a commencé par la consultation de l'industrie et est maintenant dans la phase de qualification (phase 1).

1.5.2 Les détails présentés dans le tableau 1 ci-dessous sont fournis à titre d'information seulement. Le Canada se réserve le droit de supprimer, de modifier ou d'ajouter au besoin des phases d'approvisionnement, des objectifs et des dates cibles connexes.

Tableau 1 – Processus d'approvisionnement

Étape du processus d'approvisionnement	Description	Target Date
Consultation de l'industrie (terminée)	• Trois DDRs ont été publiées sur le Service électronique d'appels d'offres du gouvernement (site Web achatsetventes.gc.ca) DDR#1:https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XU-005-38547 DDR#2: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XU-005-39080 DDR#3 : https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XU-005-39339 • Journée de l'industrie • Séances individuelles • Publication du Rapport sommaire des rétroactions et des résultats de la consultation	Terminé
Phase de qualification de l'ISQ phase 1 -étape 1	• Publier l'ISQ sur le Service électronique d'appels d'offres du gouvernement (site Web achatsetventes.gc.ca) • Recevoir et évaluer les réponses à l'ISQ afin de d'identifier les Répondants provisoirement qualifiés qui rencontrent les critères d'évaluation obligatoires et les inviter à participer au processus d'examen et d'affinement des besoins.	Printemps/ Été 2021
Phase de qualification de l'ISQ phase 1 - étape 2	• Effectuer une évaluation préliminaire de l'information de la sécurité de la chaîne d'approvisionnement (ISCA) et une évaluation de la participation, contrôle et influence de l'étranger (PCIE) pour les Répondants provisoirement qualifiés en parallèle avec le processus d'examen et d'affinement des besoins (phase 2 ci-dessous). • Création d'une liste de Répondants qualifiés qui ont réussi l'évaluation ISCA et l'évaluation PCIE pour être invités à la phase d'appel d'offres.	Printemps/ Été 2021
Phase d'examen et d'affinement des besoins (EAB) phase 2	• Fournir aux Répondants qualifiés une ébauche des documents de sollicitation des services gérés du SGPN et des CC. • Fournir aux Répondants provisoirement qualifiés l'occasion d'améliorer leur compréhension des exigences des services gérés du SGPN et des CC • Donner au Canada l'occasion d'obtenir des recommandations d'amélioration des exigences des services gérés du SGPN et des CC par les Répondants provisoirement qualifiés	Été 2021
Sollicitation (DDP) phase 3	• Envoyer la sollicitation directement à tous les Répondants qualifiés • Réception de soumissions • Évaluer les offres conformément à la DDP • Démonstration de la preuve de proposition si requise • Déterminer la liste des soumissions techniques	

	recevables • Prioriser les soumissions basées sur la méthodologie de sélection contenu dans la sollicitation.	
Phase 4 – Attribution du contrat	• Approche contractuelle agile en plusieurs étapes • Sélectionnez l'offre(s) gagnante(s) • Attribuer le(s) contrats	
Phase 5 - Mise en œuvre / Projet (s) pilote (s)	Déploiement du programme de services gérés du SGPN et des CC	

1.5.3 **Consultation de l'industrie**

Le Canada a consulté l'industrie en publiant une demande de renseignements (DDR) 1 le 20 octobre 2020, puis en organisant une activité avec l'industrie, en menant des séances individuelles et en publiant la DDR 2 le 22 février 2021 et la DDR 3 le 1er avril 2021. Le processus de consultation de l'industrie s'est terminé le 17 mai 2021.

1.5.4 **Phase de qualification : Phase 1 – Étape 1 (qualification provisoire) et étape 2 (qualification finale des Répondants provisoirement qualifiés)**

La phase de qualification de l'ISQ est la première phase du processus d'approvisionnement en plusieurs phases des services gérés du SGPN national et des caméras corporelles. Les fournisseurs sont invités à se soumettre à une sélection préalable, conformément aux modalités de la présente ISQ, afin d'être retenus comme « Répondants qualifiés » pour les phases ultérieures du processus d'approvisionnement.

1.5.4.1 **Phase 1 – Étape 1 (qualification provisoire) :** Voir la partie 4 – Procédures d'évaluation et méthode de sélection pour une explication plus détaillée des procédures d'évaluation de l'ISQ et de la méthode de sélection des Répondants qualifiés.

1.5.4.2 **Phase 1 – Étape 2 (qualification finale des Répondants provisoirement qualifiés):** Le Canada commencera l'évaluation de l'information sur la sécurité de la chaîne d'approvisionnement et l'évaluation de la participation, contrôle et influence de l'étranger dans le cadre du processus d'ISQ. L'évaluation préliminaire de l'information sur la sécurité de la chaîne d'approvisionnement et l'évaluation de la participation, contrôle et influence de l'étranger seront menées parallèlement à la phase de l'examen et de l'amélioration des besoins (EAB). Les Répondants provisoirement qualifiés peuvent être écartés à l'étape 2 de la phase de qualification s'ils ne satisfont pas aux exigences de sécurité du Canada.

1.5.5 Phase d'examen et d'affinement des besoins (phase 2)

1.5.5.1 Les objectifs de la phase d'examen et d'affinement des besoins sont notamment les suivants :

i) veiller à ce que les Répondants provisoirement qualifiés aient l'occasion d'effectuer un examen approfondi de l'ébauche des documents de demande de soumissions et de fournir des commentaires à ce sujet;

ii) obtenir des recommandations de la part des Répondants provisoirement qualifiés en vue d'améliorer l'ébauche des documents de demande de soumissions. À sa seule discrétion, le Canada décidera si des changements sont nécessaires ainsi que la nature de ces changements.

1.5.5.2 Au cours de cette phase, le Canada peut communiquer avec les Répondants provisoirement qualifiés pour obtenir des commentaires écrits sur les ébauches, et tenir des séances de travail ou des rencontres individuelles dans le but de peaufiner les documents d'invitation à soumissionner. Les détails seront communiqués en temps opportun.

i) Le gouvernement du Canada peut organiser des rencontres individuelles avec les Répondants provisoirement qualifiés après la réunion de lancement. Ces rencontres seront un lieu d'échanges permettant au Canada et aux Répondants provisoirement qualifiés d'examiner en collaboration les exigences préliminaires concernant la demande de soumissions afin que le Canada puisse affiner le contenu ainsi que la manière dont celui-ci est formulé et que les Répondants provisoirement qualifiés puissent mieux comprendre les exigences relatives au projet.

ii) Services publics et Approvisionnement Canada (SPAC) fournira au chef de projet de chaque Répondant provisoirement qualifié le calendrier préliminaire et le lieu des rencontres individuelles au moins cinq jours ouvrables avant la première réunion. En raison du calendrier serré, certaines rencontres individuelles avec des Répondants provisoirement qualifiés pourraient avoir lieu simultanément.

iii) Les rencontres individuelles se veulent des échanges ouverts et axés sur la collaboration entre les Répondants provisoirement qualifiés et le Canada. Le Canada utilisera la téléconférence en raison des restrictions sanitaires (Covid-19). La tenue de rencontres en personne n'est pas prévue. Si des rencontres individuelles ont lieu en personne, ce sera dans la région de la capitale nationale.

iv) Le nombre de représentants de chaque Répondant provisoirement qualifié pouvant assister à chaque rencontre individuelle sera fourni à une date ultérieure. Les Répondants qualifiés seront alors invités à transmettre par courriel à l'autorité contractante, dans le délai qu'elle aura stipulé, le nom, les coordonnées, le titre et le niveau d'habilitation de sécurité des représentants qui participeront à chaque rencontre individuelle.

1.5.5.3 Le Canada détermine à sa seule discrétion si les Répondants provisoirement qualifiés peuvent être autorisés à se faire accompagner aux rencontres individuelles par des représentants de sous-traitants potentiels, et les instructions à cet égard seront fournies à une date ultérieure. Toutefois, tout représentant d'un sous-traitant sera compris dans le nombre total de représentants autorisé pour ce Répondant provisoirement qualifié. Par ailleurs, les Répondants doivent être conscients que la présence d'un sous-traitant risque de compromettre la confidentialité des rencontres individuelles si le sous-traitant est également le sous-traitant potentiel d'autres Répondants qualifiés ou est lui-même un Répondant qualifié. Le gouvernement du Canada n'est pas tenu d'informer un Répondant provisoirement qualifié qu'un sous-traitant travaille avec un ou plusieurs autres Répondants provisoirement qualifiés.

1.5.5.4 Compte tenu de l'esprit de collaboration sur lequel reposeront les rencontres individuelles, la teneur des rencontres avec un Répondant provisoirement qualifié pourrait être assez différente de celle d'une rencontre avec un autre Répondant provisoirement qualifié, même si le thème général de la discussion est le même. Tous les Répondants provisoirement qualifiés pourront poser des questions durant ces rencontres. Les renseignements communiqués à un Répondant

provisoirement qualifié en réponse à des questions orales posées au cours de rencontres individuelles ne seront pas automatiquement fournis aux autres Répondants provisoirement qualifiés. Il incombe plutôt à chacun des Répondants provisoirement qualifiés de déterminer les renseignements dont il a besoin et de poser des questions en conséquence.

1.5.5.5 À la seule discrétion du Canada, d'autres rencontres individuelles peuvent être organisées ponctuellement, à l'initiative du Canada ou à la demande d'un Répondant provisoirement qualifié, si l'autorité contractante juge que la demande est raisonnable et concorde avec le calendrier du projet. Le Canada peut, à sa seule discrétion, examiner les demandes de rencontres supplémentaires de tous les Répondants provisoirement qualifiés. Cependant, en raison du moment des différentes demandes ou de leur objet, certaines pourraient être acceptées et d'autres non.

1.5.5.6 Si un Répondant provisoirement qualifié est écarté à l'issue de l'étape 2 de la phase 1, et que la phase d'affinement des besoins n'est pas terminée, le Répondant provisoirement qualifié doit mettre un terme à ses activités dans le cadre de cette phase dès qu'il en est informé par le Canada.

1.5.5.7 Le Canada se réserve le droit, à sa seule discrétion, de ne pas effectuer la phase d'affinement des besoins et de passer à la phase suivante du processus d'approvisionnement. Le Canada se réserve également le droit de modifier les exigences et d'incorporer tout changement dans les futurs documents de demande de soumissions.

1.5.6 **Phase 3 – Présentation des soumissions**

Cette phase comprend ce qui suit :

1.5.6.1 l'envoi d'une demande de soumissions aux Répondants qualifiés pour l'acquisition des services gérés du SGPN national et des caméras corporelles;

1.5.6.2 la réception et l'évaluation des soumissions présentées en réponse à la demande de soumissions;

1.5.6.3 la détermination de la ou des soumissions recevables et du ou des soumissionnaires qui les ont présentées conformément aux exigences énoncées dans la demande de soumissions.

1.5.6.4 L'approche suivante concernant la phase n'a pas encore été arrêtée et sera définie dans le document de demande de soumissions. La phase de présentation des soumissions peut inclure ou non une exigence de démonstration de la validité de la proposition.

1.5.7 **Phase 4 : Attribution du contrat**

1.5.7.1 L'objectif de la phase d'attribution du contrat est l'attribution par le Canada d'un ou de plusieurs contrats à un ou plusieurs des soumissionnaires ayant déposé une soumission recevable qui se classent au premier rang, conformément à la demande de soumissions pour l'acquisition des services gérés du SGPN national et des caméras corporelles.

1.5.7.2 Approche de contrat agile en plusieurs phases : Le Canada peut attribuer plusieurs contrats à des soumissionnaires classés au premier rang pour la mise en œuvre d'un projet pilote limité de déploiement du SGPN et des caméras corporelles au cours d'une période stipulée conformément aux travaux qui seront décrits dans l'énoncé des travaux de la demande de soumissions. Il est

prévu qu'un contrat à long terme sera attribué en fonction du rendement du ou des entrepreneurs pendant le projet pilote. Les détails de l'approche seront exposés dans la demande de soumissions.

1.6 Accords commerciaux, Ententes sur les revendications territoriales globales et Accord du Nunavut

1.6.1 Accords commerciaux

1.6.1.1 Le présent processus d'approvisionnement est assujetti à l'Accord de libre-échange canadien (ALEC). De plus, il est assujetti aux dispositions relatives à l'approvisionnement énoncées dans les accords commerciaux internationaux suivants :

- Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC)
- Accord de continuité commerciale Canada–Royaume-Uni
- Accord de libre-échange Canada-Corée (ALECC)
- Accord de libre-échange canadien (ALEC)
- Accord économique et commercial global (AECG)
- Accord de libre-échange Canada-Ukraine (ALICU)

1.6.1.2 Objectifs légitimes et dispositions de non-divulgation

Pour assurer que le présent processus d'approvisionnement permet à la GRC d'atteindre ses objectifs légitimes consistant à protéger la sécurité nationale, la sécurité publique, l'ordre public et la vie humaine, le Canada prendra des mesures pour la protection des données du Canada. Le Canada a déterminé des exigences techniques et des exigences en matière de sécurité (décrites dans la présente ISQ, et dans toute DDP à venir) qui constituent des mesures qui doivent être prises pour permettre à la GRC de protéger la sécurité nationale, la sécurité publique, l'ordre public et la vie humaine. En cas d'incompatibilité entre ces mesures et les obligations découlant des accords commerciaux applicables, le Canada s'appuie sur les dispositions relatives aux objectifs légitimes de ces accords commerciaux. De plus, le Canada s'appuie sur les dispositions de non-divulgation de chacun des accords commerciaux, selon lesquelles le Canada n'est pas tenu de communiquer des renseignements confidentiels lorsque cette divulgation serait contraire à l'intérêt public.

Ces mesures permettent d'exécuter un processus concurrentiel qui offrira le meilleur rapport qualité-prix à l'État et aux Canadiens, tout en offrant les mesures de protection de la sécurité nécessaires à la GRC pour atteindre ses objectifs légitimes.

1.6.2 Ententes sur les revendications territoriales globales (ERTG)

La présente ISQ a pour but d'établir une liste de Répondants qualifiés qui seront autorisés à répondre à une demande de soumissions pour la satisfaction des besoins décrits dans cette ISQ dans des régions comprenant celles visées par les ententes sur les revendications territoriales globales. S'il y a lieu, les ententes sur les revendications territoriales globales applicables seront déterminées à la phase de présentation des soumissions.

1.6.3 Accord sur les revendications territoriales du Nunavut

La présente ISQ a pour but d'établir une liste de Répondants qualifiés qui seront autorisés à répondre à une demande de soumissions pour la satisfaction des besoins décrits dans cette ISQ dans des régions comprenant celles visées par l'*Accord sur les revendications territoriales du Nunavut*. L'applicabilité de l'*Accord* sera indiquée à la phase de présentation des soumissions.

Des conseils et une orientation concernant l'application des modalités d'approvisionnement du gouvernement dans la région du Nunavut et concernant la Directive sur les marchés de l'État, incluant les baux immobiliers, dans la région du Nunavut peuvent être obtenus en communiquant avec la Division de la participation autochtone à l'approvisionnement du Secteur de la politique stratégique à : PA Contrats Nunavut/AP Nunavut Contracts (TPSGC/PWGSC)

1.7 Exigences relatives à la sécurité de l'ISQ

1.7.1 Les exigences relatives à la sécurité pour l'ISQ et les exigences futures prévues en matière de sécurité associées à ce marché se trouvent dans la **partie 6 – Exigences relatives à la sécurité**.

1.7.2 Pour en savoir plus sur les enquêtes de sécurité concernant le personnel et les organisations ou sur les clauses de sécurité, les Répondants sont invités à consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

1.8 Compte rendu (ISQ)

Les fournisseurs peuvent demander un compte rendu des résultats du processus de demande d'arrangements en matière d'approvisionnement. Les fournisseurs devraient en faire la demande au responsable de l'arrangement en matière d'approvisionnement dans les 15 jours ouvrables, suivant la réception des résultats du processus ISQ. Le compte rendu peut être fourni par écrit, par téléphone ou par conférence vidéo à la discrétion du Canada.

1.9 Conflit d'intérêt

1.9.1 Les Répondants doivent se référer aux dispositions sur les conflits d'intérêts à l'article 18 des CCUA 2003 (2020-05-28), Instructions uniformisées - biens ou services - besoins concurrentiels (tel que modifié par l'article 2.1.2) disponible respectivement sur le site Web de TPSGC suivant:

- https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat/1/2003/25.

1.9.2 Sans limiter de quelque manière que ce soit les dispositions décrites au point 1.9.1 ci-dessus, les Répondants sont informés que le Canada a retenu l'aide d'entrepreneurs et de ressources du secteur privé suivants qui ont fourni des services, y compris l'examen du contenu en préparation de la présente ITQ et / ou avoir eu, ou a pu avoir accès à des informations relatives à cette ITQ ou à d'autres documents liés au système national de gestion des preuves numériques et aux caméras corporelles::

Entrepreneurs	Ressources
Modis Canada Inc.	Vojinovic, Dragana
	Duffy, Kristen
PricewaterhouseCoopers LLP	Kuta, Dave
	Kaegi, Erin
	deCotret, Michael
	Lesarge, Aaron
	Lotan, Ryan
	Young, Rachel
Veritaaq Technology House Inc.	Osipenko, Larry

1.9.3 Toute réponse reçue de l'un des entrepreneurs susmentionnés, que ce soit en tant que seul Répondant, en coentreprise ou en tant que sous-traitant d'un Répondant; ou pour laquelle l'une des ressources susmentionnées a fourni une contribution à la réponse, sera considérée comme contraire aux clauses de conflit d'intérêts identifiées au sous-paragraphe 1.9.1, et la réponse sera déclarée non recevable.

1.9.4 En soumettant une réponse, le Répondant déclare qu'il ne se considère pas en conflit d'intérêts ni ne bénéficie d'un avantage indu. Le Répondant reconnaît qu'il est à la seule discrétion du Canada de déterminer s'il existe un conflit d'intérêts, un avantage injuste ou une apparence de conflit d'intérêts ou d'avantage injuste.

1.9.5 L'expérience acquise par un Répondant qui fournit ou a fourni les biens et services décrits dans l'ITQ (ou des biens ou services similaires) au Canada ne sera pas, en soi, considérée par le Canada comme ayant un avantage indu ou créant un conflit d'intérêts. Chaque Candidat reste toutefois soumis aux critères établis ci-dessus.

1.9.6 Si le Canada a l'intention de disqualifier une réponse en vertu de cette section, l'Autorité Contractante informera le Répondant et lui donnera l'occasion de présenter des observations avant de prendre une décision finale. Les Répondants qui ont des doutes sur une situation particulière doivent contacter l'autorité contractante avant la date de clôture.

1.10 Surveillant de l'équité

1.10.1 Le Canada a retenu les services de RFPSolutions Inc. pour agir en tant que tiers indépendant surveillant de l'équité (SÉ) pour le processus d'approvisionnement du système national de gestion des preuves numériques et des caméras corporelles. Le rôle du SÉ est de fournir une attestation d'assurance sur l'équité, l'ouverture et la transparence des activités surveillées.

1.10.2 Le surveillant de l'équité ne fera pas partie de l'équipe d'évaluation, mais aura accès à toute réponse soumise en réponse à cette ISQ et à toute correspondance connexe reçue par le Canada conformément à cette ISQ. Le SÉ observera l'évaluation des réponses de l'ISQ en ce qui concerne le respect par le Canada du processus d'évaluation décrit dans cette ISQ et observera les comptes rendus des réponses

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES RÉPONDANTS

2.1 Instructions, clauses et conditions uniformisées

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

2.1.2 Le guide CCUA 2003 (2020-05-28*)* Instructions uniformisées - biens ou services – besoins concurrentiels (comme modifié dans cette section 2.1.2), est incorporé par renvoi à l'ISQ et en fait partie intégrante comme d'il y était expressément reproduit, mis à part le fait que :

i) l'expression « demande de soumissions » doit être remplacée par « invitation à se qualifier »;
ii) le terme « soumission » doit être remplacé par « réponse » ;
iii) le terme « soumissionnaire » doit être remplacé par « Répondant » ;
iv) Le paragraphe 5 (4), qui traite d'une période de validité, ne s'applique pas, étant donné que l'ISQ invite simplement les Répondants à se qualifier. À moins que le Répondant n'informe l'autorité contractante par écrit de son désir de retirer sa réponse, le Canada supposera qu'il tient toujours à se qualifier.
v) Le titre de la section 10 est modifié comme suit : « Capacité juridique, et information sur la propriété et le contrôle »; le premier paragraphe est numéroté 1 et les éléments suivants sont ajoutés :

2. Le fournisseur doit fournir, à la demande de l'autorité contractante, les renseignements suivants et tout autre renseignement requis concernant la propriété et le contrôle du fournisseur, de ses propriétaires, de sa direction, de toute personne morale et société de personnes qui lui est liée :

a) Un organigramme sur lequel figurent toutes les personnes morales et sociétés de personnes qui sont liées au fournisseur ;

b) Une liste de tous les intervenants ou partenaires du fournisseur, selon le cas; si le fournisseur est une filiale, les renseignements doivent être fournis pour chaque société mère (personne morale ou société de personnes), et ce, jusqu'à l'ultime propriétaire;

c) Une liste de tous les dirigeants et administrateurs du fournisseur, comprenant l'adresse de leur domicile, leurs date et lieu de naissance, et leur(s) citoyenneté(s); si le fournisseur est une filiale, ces renseignements doivent être fournis pour chaque société mère (personne morale ou société de personnes), et ce, jusqu'à l'ultime propriétaire.

3. Si le fournisseur est une coentreprise, ces renseignements doivent être fournis pour chaque membre de la coentreprise. L'autorité contractante peut également demander que ces renseignements soient fournis pour tout sous-traitant mentionné dans la réponse.

4. Aux fins d'application de cette section, une personne morale ou une société de personnes sera considérée comme liée à une autre partie :

a) S'il s'agit de « personnes liées » ou de « personnes affiliées » aux termes de la *Loi de l'impôt sur le revenu du Canada*;

b) Si les entités entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire) ou ont entretenu une telle relation au cours des deux dernières années précédant la date de clôture;

c) Si les entités n'ont pas de lien de dépendance entre elles ou chacune d'elles n'a pas de lien de dépendance avec le même tiers.

2.1.3 En soumettant une réponse, le Répondant confirme qu'il s'engage à respecter toutes les modalités de la présente ISQ, y compris celles incorporées par renvoi.

2.1.4 En cas de divergence entre les dispositions du présent document et de tout autre document qui y est incorporé par renvoi comme susmentionné, le présent document l'emporte.

2.2 Présentation des réponses

2.2.1 Les réponses doivent être présentées uniquement à l'Unité de réception des soumissions de TPSGC **par l'entremise du service Connexion postel** au plus tard à la date et à l'heure indiquées à la page 1 de l'ISQ.

2.2.2 Pour les Répondants qui doivent s'inscrire à Connexion postel pour la clôture de l'ISQ à l'Unité de réception des soumissions de la région de la capitale nationale (RCN), l'adresse courriel est la suivante :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

2.2.3 Les Répondants intéressés doivent s'inscrire quelques jours avant la date de clôture de l'ISQ.

2.2.4 Aucune réponse transmise directement à cette adresse de courriel ne sera acceptée. Cette adresse courriel doit être utilisée pour ouvrir une conversation Connexion postel, comme indiqué dans les Instructions uniformisées 2003 (2020-05-28) du CCUA (tel que modifié dans cette section 2.1.2),, ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

2.2.5 En raison de la nature de l'ISQ, les soumissions transmises par télécopieur à TPSGC ne seront pas acceptées.

2.2.6 Aucune réponse ne doit être envoyée directement à l'autorité contractante de TPSGC.

2.3 Demandes de renseignements

2.3.1 Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 5 jours civils avant la date de clôture de l'ISQ. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

2.3.2 Les Répondants doivent acheminer les demandes de renseignements au sujet de l'ISQ :

Autorité contractante
Travaux publics et Services gouvernementaux Canada

Nom : Kent Cummings

Courriel : TPSGC.PACCSGPN-APBWCDEMS.PWGSC@tpsgc-pwgsc.gc.ca

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

2.4 Présentation d'une seule réponse

2.4.1 L'« invitation à se qualifier » (ISQ) est une demande de manifestations d'intérêt et non un appel d'offres ou une demande de soumissions. Aucune période de validité des soumissions ne s'applique étant donné qu'une ISQ invite seulement les Répondants à se qualifier. Le Canada présumera que tous les Répondants souhaitent se qualifier, à moins qu'ils ne se retirent par écrit. Si un Répondant comprend plus d'une entité, le retrait de toute entité du Répondant pendant la phase d'ISQ entraînera le retrait de la réponse de ce dernier.

2.4.2 Un Répondant peut être un particulier, une entreprise individuelle, une société, une société de personnes ou une coentreprise.

2.4.3 Chaque Répondant (entités liées comprises) ne pourra se qualifier qu'une seule fois. Si un Répondant ou une entité liée participe à plusieurs réponses (par participer, on entend faire partie du Répondant, et non être un sous-traitant), le Canada lui accordera deux (2) jours ouvrables pour indiquer la réponse unique que le Canada devra examiner. Si ce délai n'est pas respecté, toutes les réponses concernées pourraient être déclarées irrecevables ou le gouvernement du Canada pourrait choisir, à sa discrétion, laquelle des réponses il évaluera.

2.4.4 Aux fins du présent article, peu importe où les entités ont été constituées en société ou formées juridiquement (qu'il s'agisse de personnes physiques, de sociétés commerciales, de sociétés de personnes ou autres), une entité est considérée comme « liée » à un Répondant dans les cas suivants :

2.4.4.1 s'il s'agit de la même personne morale que le Répondant (c.-à-d. la même personne physique, société commerciale, société de personnes, société à responsabilité limitée, etc.);

2.4.4.2 si l'entité et le Répondant sont des « personnes liées » ou des « personnes affiliées » aux termes de la *Loi de l'impôt sur le revenu* du Canada;

2.4.4.3 si l'entité et le Répondant entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire) ou ont entretenu une telle relation au cours des deux années ayant précédé la clôture de l'ISQ;

2.4.4.4 si l'entité et le Répondant ont tout autre lien de dépendance entre eux ou avec le même tiers.

2.4.4.5 Les sous-traitants peuvent ne pas être autorisés à participer à la phase d'examen et d'affinement des besoins avec le Répondant provisoirement qualifié pour lequel ils effectueront des travaux de sous-traitance.

2.4.4.6 Si une personne, une entreprise individuelle, une société ou une société de personnes est un Répondant dans le cadre d'une coentreprise, elle ne peut pas soumettre une autre réponse seule ni dans le cadre d'une autre coentreprise.

Exemple 1 : À lui seul, le fournisseur A n'a pas toute l'expérience requise par l'ISQ. Toutefois, le fournisseur B a l'expérience qui manque au fournisseur A. Si le fournisseur A et le fournisseur B décident de s'associer pour soumettre une réponse ensemble en tant que coentreprise, ils sont considérés ensemble comme deux entités qui constituent le Répondant. Ni le fournisseur A ni le fournisseur B ne peuvent s'associer à un autre fournisseur pour soumettre une réponse distincte, parce que l'un et l'autre font déjà partie d'un Répondant.

Exemple 2 : Le fournisseur X est un Répondant. La filiale du fournisseur X, le fournisseur Y, décide de s'associer au fournisseur Z pour soumettre une réponse en tant que coentreprise. Les fournisseurs Y et Z, ainsi que le fournisseur X, seront tous invités à déterminer laquelle des deux réponses le Canada devra prendre en considération. Les deux réponses ne peuvent pas être soumises parce que le fournisseur Y est lié au fournisseur X en tant que société affiliée.

2.4.4.7 En soumettant une réponse, le Répondant atteste qu'il ne considère pas qu'il est lié à un autre Répondant.

2.4.4.8 L'autorité contractante peut tout de même exiger qu'une ou plusieurs des entités constituant un Répondant présentent une attestation ou un avis juridique indiquant si elles sont liées ou non à un autre Répondant et expliquant pourquoi.

2.5 Lois applicables

2.5.1 L'invitation à se qualifier (ISQ) seront interprétés et régis selon les lois en vigueur en Ontario et les relations entre les parties seront déterminées par ces lois.

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

2.6 Langue

2.6.1 Les Répondants sont priés d'indiquer, par écrit, dans le formulaire 1 : Formulaire de la déclaration et de soumission du Répondant, laquelle des deux (2) langues officielles du Canada (français ou anglais) ils choisissent d'utiliser pour leurs communications futures avec le Canada concernant la présente ISQ et toute phase ultérieure du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES RÉPONSES

3.1 Instructions pour la préparation des réponses

Les Répondants doivent soumettre leur réponse par voie électronique par l'entremise du système Connexion postel dans une seule soumission conformément au paragraphe 2 de la section 08 du guide CCUA 2003 (2020-05-28) Instructions uniformisées, tel que modifié dans la présente ISQ. Le système Connexion postel a une limite de 1 Go par message individuel affiché et de 20 Go par conversation. La réponse devrait être présentée en sections distinctes comme suit :

(i) Section I : Réponse de qualification de l'ISQ
(ii) Section II : Attestations et renseignements supplémentaires

Les prix ne sont pas requis et ne doivent pas être inclus dans la réponse.

3.2 Section I : Réponse de qualification de l'ISQ

Dans leur réponse de qualification à l'ISQ, les Répondants doivent expliquer comment ils prévoient répondre aux exigences obligatoires. Ils doivent démontrer leur capacité de satisfaire à toutes les exigences obligatoires et décrire de façon complète, concise et claire leur approche pour satisfaire aux exigences obligatoires.

Les Répondants doivent soumettre leur réponse de qualification comme suit :

3.2.1 Formulaire de présentation **:** Les Répondants devraient inclure le formulaire de présentation et déclaration du répondant (**formulaire 1**) dans leur réponse. Si le Canada considère que les renseignements requis par le formulaire de présentation des réponses sont incomplets ou doivent être corrigés, le Canada accordera au Répondant la chance de compléter ou de corriger ces renseignements. Pendant la période d'évaluation, il est obligatoire de fournir les renseignements lorsqu'ils sont demandés. Si le Répondant n'a pas fourni les renseignements demandés pendant la période fixée par l'autorité contractante, sa réponse sera déclarée non recevable.

3.2.2 Critères obligatoires pour se qualifier **:** Les Répondants doivent justifier leur conformité aux critères obligatoires qui sont évalués à l'annexe B – Critères d'évaluation obligatoires, et traiter ces critères de façon claire et suffisamment approfondie. Chaque critère obligatoire doit être traité avec suffisamment de détails pour permettre à l'équipe d'évaluation de vérifier la conformité du Répondant. Il ne suffit pas de reprendre simplement les énoncés contenus dans l'ISQ. Pour faciliter l'évaluation de la réponse, le Canada demande aux Répondants de reprendre les critères d'évaluation dans le même ordre que celui de l'annexe B – Critères d'évaluation obligatoires. Pour éviter les recoupements, les Répondants peuvent faire des renvois à diverses sections de leur réponse en indiquant le numéro du paragraphe et de la page où le critère est déjà traité. Lorsque le Canada détermine que la justification n'est pas complète et que le Canada détermine également, à sa seule discrétion, que la justification n'a pas été corrigée par le biais du processus de conformité des soumissions en phases (PCSP) énoncé à l'article 4.2 - Évaluation des réponses - Processus de conformité des soumissions en phases, ou n'est pas une correction admissible en vertu du PCSP, le Répondant sera considéré comme non recevable.

3.2.3 Coordonnées des références de projet (Formulaire 2 : Formulaire de vérification des projets cités en référence): Le Répondant doit fournir des références de projet pour chaque description d'expérience de projet fournie dans sa réponse afin de démontrer l'expérience requise dans l'annexe B –- Critères d'évaluation obligatoires. La personne-ressource de chaque projet cité en

référence doit confirmer, à la demande du Canada, les faits indiqués dans la réponse du Répondant relativement au projet pour lequel elle est citée comme référence, conformément à l'annexe B – Critères d'évaluation obligatoires.

i) Les Répondants sont priés de soumettre un Formulaire de vérification des projets cités en référence dûment rempli (formulaire 2) pour chaque projet cité en référence, conformément à l'annexe B– Critères d'évaluation obligatoires.

ii) Si les renseignements demandés dans ce formulaire n'accompagnent pas la réponse à l'ISQ, ils doivent être fournis sur demande de l'autorité contractante dans le délai précisé.

iii) Le Canada peut communiquer avec la personne-ressource fournie pour le projet cité en référence afin de valider l'information fournie dans la réponse du Répondant.

3.2.4 Évaluation préliminaire de l'intégrité de la chaîne d'approvisionnement (ICA): Les Répondants provisoirement qualifiés seront tenus de soumettre le formulaire 5 des «Informations sur la sécurité de la chaîne d'approvisionnement» (ISCA) pour une évaluation préliminaire par le Canada en ce qui concerne l'intégrité de la chaîne d'approvisionnement lorsqu'ils seront avisés par le Canada. Le Canada prévoit actuellement que cela aura lieu à l'étape 2 de la phase de qualification de l'ISQ (phase 1) et de la phase d'examen et d'affinement des besoins (phase 2). Le processus d'évaluation préliminaire ICA est décrit à l'annexe D - Processus d'évaluation des informations sur la sécurité de la chaîne d'approvisionnement . Veuillez-vous référer à l'annexe D et la partie 6 pour l'évaluation préliminaire de l'ICA.

3.2.5 Évaluation de la PCIE: Les Candidats provisoirement qualifiés seront tenus de soumettre des informations pour l'évaluation de la participation, contrôle et influence de l'étranger (PCIE). Les Répondants provisoirement qualifiés seront contactés directement par le bureau du programme de sécurité des contrats de TPSGC PCIE pour soumettre l'information. Ne pas fournir les informations requises dans le délai spécifié par le Canada entraînera leur disqualification. Veuillez-vous référer à la partie 6 pour les exigences PCIE.

3.3 Section II: Attestations et renseignements supplémentaires

Les Répondants doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5 - Attestations.

PARTIE 4 - PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

4.1.1 Il y a deux étapes dans le processus d'évaluation:

4.1.1.1 Étape 1: Les réponses seront évaluées conformément à l'ensemble des exigences de l'ISQ, y compris l'annexe B - Critères d'évaluation obligatoires, à l'exception de l'évaluation ISCA et PCIE. Les Répondants qualifiés à l'étape 1 seront avisés et deviendront des Répondants provisoirement qualifiés.

4.1.1.2 Étape 2: Les Répondants provisoirement qualifiés seront invités à effectuer une évaluation ISCA préliminaire décrite à l'annexe D et une évaluation PCIE en parallèle avec l'examen et le raffinement des exigences. Les détails sur l'évaluation PCIE seront fournis aux Répondants provisoirement qualifiés au moment de l'évaluation.

(i) Le Canada demandera aux Répondants provisoirement qualifiés de fournir des informations, y compris leur structure organisationnelle, leur chaîne d'approvisionnement et des informations financières, ainsi que leurs entités de chaîne d'approvisionnement qui seront utilisées dans l'exécution du contrat.

(ii) Le Centre canadien de la sécurité et le Programme de sécurité des contrats lanceront ces évaluations directement avec les Répondants provisoirement qualifiés. Le Canada se réserve le droit de poursuivre ces processus d'évaluation pour tout sous-traitant ou sous-processeur dans le cadre du processus de demande de propositions.

4.1.2 Une équipe d'évaluation composée de représentants du Canada et d'experts-conseils indépendants évaluera les réponses. Le Canada peut faire appel à des experts-conseils indépendants ou à des personnes-ressources du gouvernement pour évaluer les réponses. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation. En soumettant leur réponse, les Répondants consentent à ce qu'elle soit communiquée aux experts-conseils tiers engagés par le Canada, sous réserve que le Canada signe avec ces derniers l'engagement en matière de confidentialité.

4.1.3 La conformité de chaque réponse à chacune des exigences obligatoires de la présente ISQ sera évaluée. Le Répondant pourrait avoir l'occasion de fournir des renseignements supplémentaires pour justifier la conformité à l'exigence obligatoire, conformément au processus de conformité des soumissions par étapes décrit dans l'article 4.2 ci-dessous.

4.1.4 Les critères d'évaluation obligatoires sont décrits à l'annexe B − Critères d'évaluation obligatoires.

4.1.5 Lorsque le Canada évalue les réponses, il peut :

4.1.5.1 communiquer avec l'une ou l'ensemble des personnes-ressources citées en référence pour les projets par les Répondants pour vérifier et attester l'exactitude des renseignements fournis par ces derniers;

4.1.5.2 demander des précisions ou vérifier l'exactitude d'une partie ou de la totalité des renseignements fournis par les Répondants en réponse à l'ISQ.

4.1.6 Outre les périodes fixées dans l'ISQ:

4.1.6.1 **Demandes de précisions** : Si le Canada demande des précisions au Répondant au sujet de sa réponse ou s'il veut vérifier celle-ci, le Répondant disposera d'un délai de deux (2) jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. Si le Répondant ne respecte pas ce délai, sa réponse sera déclarée non recevable.

4.1.6.2 **Demandes de renseignements supplémentaires :** Si le Canada a besoin de renseignements supplémentaires pour faire ce qui suit conformément à la section intitulée « Déroulement de l'évaluation » du guide CCUA 2003 (2020-05-28), Instructions uniformisées - biens ou services - besoins concurrentiels (tel que modifié par la section 2.1.2):

A. vérifier tout renseignement fourni par le Répondant dans sa réponse;
B. communiquer avec une ou plusieurs des références citées par le Répondant (p. ex. personne-ressource indiquée pour chaque projet) dans le but de valider les renseignements fournis par le Répondant.

4.1.6.3 **Prolongation du délai :** Si le Répondant a besoin de plus de temps, l'autorité contractante pourra le lui accorder, à sa seule et entière discrétion.

4.1.7 Seuls les documents de référence inclus dans la réponse du Répondant, ou fournis à titre de précisions à la demande de l'autorité contractante, seront évalués ou considérés. Il est de l'entière responsabilité du Répondant de fournir suffisamment de renseignements pour assurer une évaluation adéquate de sa réponse.

4.1.8 Le Canada se réserve le droit de réévaluer la qualification de n'importe quel Répondant qualifié à tout moment au cours du processus d'approvisionnement. Si des renseignements mettant en question les qualifications d'un Répondant qualifié dans le cadre de la présente ISQ sont signalés au gouvernement du Canada, ce dernier pourra évaluer de nouveau ce Répondant. Le cas échéant, le Canada pourrait demander plus de renseignements. Si le Répondant qualifié ne les fournit pas dans les cinq jours ouvrables (ou suivant une plus longue période déterminée par l'autorité contractante), le Canada peut disqualifier le Répondant qualifié.

4.1.9 Les Répondants non retenus ne pourront pas participer aux étapes ultérieures du processus d'approvisionnement ni être évalués de nouveau à cette fin, à moins que le Canada décide, à sa seule discrétion, que les circonstances nécessitent une nouvelle évaluation.

4.1.10 Le Canada se réserve le droit de lancer, à son gré, une seconde vague de qualification auprès des Répondants non retenus si, de l'avis du gouvernement du Canada, la première n'a pas permis de rassembler un nombre suffisant de Répondants qualifiés. Les Répondants qualifiés au cours de la première vague n'ont pas besoin de se qualifier de nouveau, à moins que le Canada, à seule discrétion, en décide autrement.

4.1.11 Si le Canada offre aux Répondants non retenus une deuxième occasion de se qualifier, il leur fera tous parvenir par écrit, la même journée, les raisons pour lesquelles ils ne se sont pas qualifiés au cours de la première vague.

4.1.12 Les Répondants qui ne se qualifient pas à la suite de la seconde vague effectuée par le Canada ne pourront pas participer ou être évalués de nouveau pour les étapes ultérieures du processus d'approvisionnement.

4.2 Évaluation des réponses - Processus de conformité des soumissions par phases (PCSP)

Le processus de conformité des soumissions par phases s'appliquera à tous les critères d'évaluation obligatoires dans l'annexe B.

4.2.1 Généralités

4.2.1.1 Sans égard à tout examen effectué par le Canada du PCSP, les Répondants sont et resteront les seuls responsables de l'exactitude, de l'uniformité et de l'exhaustivité de leurs réponses, et le Canada n'engage, conformément à cet examen, aucune obligation ou responsabilité de relever les erreurs ou omissions dans les réponses ou dans les réponses d'un Répondant à une communication du Canada ni ne s'engage à indiquer ces erreurs ou omissions.

Le Répondant reconnaît que les examens du PCSP sont préliminaires et n'empêchent pas qu'une réponse soit jugée non recevable, et ce, même pour les exigences obligatoires qui ont fait l'objet d'un examen et même si la réponse avait été jugée recevable. Le Canada peut juger qu'une réponse ne répond pas à une exigence obligatoire à n'importe quelle étape de l'évaluation.

Le Répondant reconnaît également que sa réponse à un avis ou à un rapport d'évaluation de la conformité (REC) (ces termes sont définis plus bas) ne rendra pas obligatoirement sa réponse conforme aux exigences obligatoires qui font l'objet de l'avis ou du REC, et pourrait rendre sa réponse non conforme à d'autres exigences obligatoires.

4.2.1.2 Le Canada peut, à sa discrétion et à tout moment, demander et accepter de l'information du Répondant pour corriger des erreurs ou des omissions de nature administrative dans la réponse, et peut considérer que cette information fait partie de la réponse; p. ex. une signature manquante, une case non cochée dans un formulaire, une erreur de format ou de forme, l'omission de l'accusé de réception, du numéro d'entreprise – approvisionnement ou les coordonnées des personnes-ressources, comme les noms, les adresses et les numéros de téléphone. Cela ne limite pas le droit du Canada d'exiger ou d'accepter tout renseignement après la date de clôture de l'ISQ lorsque l'ISQ le permet expressément. Le Répondant disposera du délai précisé par écrit par le Canada pour fournir la documentation nécessaire. Si le Répondant ne respecte pas ce délai, sa réponse sera déclarée non recevable.

4.2.1.3 Le PCSP ne limite pas les droits du Canada en vertu du CCUA 2003 (2020-05-28) Instructions uniformisées – biens ou services – besoins concurrentiels (tel que modifié à l'article Article 2.1.2), ni le droit du Canada de demander ou d'accepter toute information pendant la période de demande de soumissions ou après la date de clôture de l'ISQ dans des circonstances où cette dernière le permet expressément, ou dans les circonstances décrites au sous-paragraphe 4.4.1.2.

4.2.1.4 Le Canada enverra un avis ou un REC selon la méthode de son choix et à sa discrétion absolue. Le Répondant doit soumettre sa réponse par la méthode indiquée dans l'avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure qu'elles ont été livrées au Canada par la méthode indiquée dans l'avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'avis ou le REC. Un avis ou un REC, envoyé par le Canada au Répondant à l'adresse fournie par celui-ci dans la réponse ou conformément à la réponse est réputé avoir été reçu par le Répondant à la date à laquelle il a été envoyé par le Canada. Le Canada n'est pas responsable de la réception tardive d'une réponse par le Canada, quelle qu'en soit la cause.

4.2.2 Réponse de qualification à l'ISQ

4.2.2.1 Le Canada étudiera la réponse afin de vérifier que le Répondant satisfait à l'ensemble des critères obligatoires d'admissibilité. Les critères obligatoires d'admissibilité sont tous des critères d'évaluation obligatoires décrits dans la présente ISQ comme faisant partie du PCSP. Cet examen ne déterminera pas si la réponse respecte toute norme ou répond à toutes les exigences de l'ISQ.

4.2.2.2 Le Canada enverra un avis écrit au Répondant (REC) indiquant les critères obligatoires d'admissibilité auxquels la réponse n'a pas satisfait. Un Répondant dont la réponse a été jugée conforme aux exigences recevra un REC, attestant que sa réponse a été jugée conforme aux exigences. Un tel Répondant ne doit pas être autorisé à présenter de réponse au REC.

4.2.2.3 Le Répondant dispose de la période précisée dans le REC (la « période de correction ») pour remédier au défaut de satisfaire à tout critère obligatoire d'admissibilité indiqué dans le REC en fournissant au Canada, par écrit, des renseignements supplémentaires ou différents ou des précisions en réponse au REC. Le Canada ne prendra pas en compte les réponses reçues après la fin de la période de correction, sauf dans les circonstances et selon les modalités expressément prévues dans le REC.

4.2.2.4 La réponse du Répondant doit aborder uniquement les critères obligatoires d'admissibilité précisés dans le REC qui n'ont pas été respectés, et doit comprendre uniquement les renseignements qui sont nécessaires pour les respecter. Les renseignements supplémentaires fournis par le Répondant qui ne servent pas à déterminer la conformité à ces exigences ne seront pas pris en compte par le Canada, sauf lorsque la réponse aux critères obligatoires d'admissibilité précisés dans le REC entraîne nécessairement une modification consécutive dans d'autres parties de la réponse, le Répondant doit identifier ces modifications supplémentaires.

4.2.2.5 La réponse du Répondant au REC devrait préciser, dans tous les cas, le critère obligatoire d'admissibilité du REC auquel il répond, y compris l'identification de la section correspondante de la réponse originale, le libellé de la modification proposée à cette section, ainsi que le libellé et l'emplacement dans la réponse de toute autre modification consécutive qui découle nécessairement de cette modification. Pour chaque modification corrélative, le Répondant doit inclure une justification expliquant en quoi cette modification corrélative est une conséquence nécessaire de la modification proposée pour répondre au critère obligatoire d'admissibilité. Le Canada ne révisera pas la réponse du Répondant, et le défaut du Répondant de le faire, conformément au présent alinéa, est à ses propres risques. Tous les renseignements fournis doivent satisfaire aux exigences de la présente ISQ.

4.2.2.6 Toute modification à la réponse présentée par le Répondant d'une façon qui n'est pas permise par la présente ISQ sera considérée comme une nouvelle information et sera écartée. Les renseignements fournis conformément aux exigences de la présente ISQ en réponse au REC remplaceront, en totalité, uniquement la partie de la réponse initiale comme le permet cette section.

4.2.2.7 Les renseignements supplémentaires ou différents soumis par les Répondants et permis par la présente section seront considérés comme étant inclus dans la réponse, pour les besoins de déterminer si la réponse satisfait aux critères obligatoires admissibles.

4.2.2.8 Le Canada déterminera si la réponse est conforme aux exigences, en tenant compte des renseignements supplémentaires ou différents ou des précisions que le Répondant a pu fournir conformément à la présente section. Seules les réponses qui satisfont à tous les critères d'évaluation obligatoires de l'ISQ, à la satisfaction du Canada, passeront à la prochaine étape d'évaluation.

4.3 Vérification des références

4.3.1 Il incombe au Répondant de confirmer à l'avance que la personne-ressource fournie pour chaque référence de projet sera disponible pour fournir une réponse et qu'elle est disposée à fournir une référence.

4.3.2 Aux fins de cette évaluation, on pourrait procéder à des vérifications de références pour valider les renseignements contenus dans la réponse du Répondant. Si une vérification des références est requise, le Canada effectuera la vérification par écrit, par courriel. Le Canada enverra la demande de vérification des références directement à la personne-ressource du projet fourni par le Répondant. La personne-ressource disposera de cinq (5) jours ouvrables (ou d'un délai plus long qui sera précisé par écrit par l'autorité contractante) suivant la date d'envoi du courriel, pour répondre au Canada.

4.3.3 La personne-ressource devra accuser réception de la demande de vérification des références et indiquer sa volonté et sa disponibilité à effectuer la vérification en question dans les deux (2) jours ouvrables suivant l'envoi de la demande de vérification des références par le Canada. S'il n'a pas reçu la réponse requise de la personne-ressource citée en référence, le Canada en avisera le Répondant par courriel, pour lui permettre de communiquer directement avec cette personne-ressource pour s'assurer que la réponse de celle-ci parviendra au Canada dans les délais prévus. Si la personne-ressource ne répond pas à la demande du Canada dans le délai prévu, l'expérience de projet invoquée par le Répondant ne sera pas prise en considération.

4.3.4 Sans égard aux paragraphes 4.3.2 et 4.3.3, si la personne-ressource n'est pas disponible pendant la période de l'évaluation, on demandera aux Répondants de fournir les coordonnées d'une autre personne-ressource pour le même projet cité en référence. Cette possibilité ne sera offerte qu'une fois au Répondant pour chaque projet cité en référence, et ce, uniquement si la première personne-ressource n'est pas en mesure de le faire. Le processus décrit aux paragraphes 4.3.2 et 4.3.3 s'applique à la vérification des références auprès de la nouvelle personne-ressource. La première personne-ressource citée en référence, ou son remplaçant, disposera d'un total de cinq (5) jours ouvrables (ou d'un délai plus long qui sera précisé par écrit par l'autorité contractante) pour fournir une réponse, conformément au paragraphe 4.3.2.

4.3.5 En cas de contradiction entre les renseignements fournis par la personne-ressource et ceux fournis par le Répondant, on demandera au Répondant de préciser les renseignements sur le projet cité en référence dans sa réponse à l'ISQ. Le Canada évaluera les renseignements suivants dans le cadre de l'évaluation de la réponse du Répondant : les renseignements sur le projet cité en référence fournis initialement par le Répondant; les renseignements fournis par le Répondant en réponse à la demande de précisions; les renseignements fournis par la personne-ressource en lien avec le projet cité en référence.

4.3.6 Un Répondant ne respectera pas le critère obligatoire en matière d'expérience si :

4.3.6.1 la personne-ressource indiquée ne répond pas dans le délai exigé à la demande du Canada;

4.3.6.2 la personne-ressource déclare ne pas pouvoir ou vouloir fournir les renseignements demandés;

4.3.6.3 les renseignements fournis par le Répondant ne peuvent pas être vérifiés par le Canada;

4.3.6.4 l'organisme d'application de la loi est lui-même une filiale ou une autre entité qui a un lien de dépendance avec le soumissionnaire.

4.3.6.5 La vérification des références est à l'entière discrétion du Canada. Toutefois, si le Canada décide d'effectuer une vérification des références au sujet d'une des exigences obligatoires, il

l'effectuera pour chaque Répondant dont la réponse n'a pas, à ce moment-là, été déclarée non recevable.

4.4 Critères de qualification de base

4.4.1 Pour être jugée recevable, une réponse doit :

4.4.1.1 satisfaire aux qualifications et conditions s de l'ISQ;

4.4.1.2 répondre à tous les critères d'évaluation obligatoires indiqués à l'annexe B – Critères d'évaluation obligatoires.

4.4.1.3 être qualifié à la suite des évaluations de l'ISCA et du PCIE

4.4.2 Les réponses qui ne satisfont pas au sous-article 4.4.1.1 ou au sous-article 4.4.1.2 ou qui ne se qualifient pas au sous-article 4.4.1.3 seront déclarées irrecevables et rejetées.

4.4.3 Les Répondants dont les réponses sont évaluées comme respectant le sous-article 4.4.1.1 et le sous-article 4.4.1.2 seront éligibles pour participer à la phase EAB.

4.4.4 Les Répondants dont les réponses sont évaluées comme respectant le sous-article 4.4.1.1 et le sous-article 4.4.1.2 mais qui ne respectent pas le sous-article 4.4.1.3, ne seront pas autorisés à poursuivre la phase EAB et tout processus d'achat ultérieur.

4.4.5 Seuls les Répondants dont les réponses sont évaluées comme respectant les sous-articles4.4.1.1, 4.4.1.2 et 4.4.1.3 seront sélectionnés comme «Répondants qualifiés» et seront invités à participer à toutes phases subséquentes du processus d'approvisionnement.

4.4.6 L'autorité contractante informera, par écrit, chaque Répondant s'il a été qualifié pour les prochaines étapes du processus d'approvisionnement une fois que chaque phase ou étape est complétée.

4.4.7 Le gouvernement du Canada publiera également la liste des Répondants qualifiés sur le site Achatsetventes.gc.ca.

4.4.8 Si, après la phase de l'ISQ, le nombre de Répondants qualifiés n'est pas suffisant pour assurer un processus d'approvisionnement concurrentiel lors des phases subséquentes, le Canada se réserve le droit d'annuler toute phase subséquente du processus d'approvisionnement ou de procéder à une deuxième vague de qualification conformément au sous-article 4.1.10 afin de modifier les exigences de la phase de l'ISQ et de publier de nouveau la demande de soumissions selon la même approche ou une approche différente.

4.4.9 Cette ISQ peut être annulée si moins de 3 réponses sont reçues ou s'il y a moins de 3 répondants qualifiés.

PARTIE 5 – ATTESTATIONS

Les Répondants doivent fournir les attestations requises afin de devenir des fournisseurs qualifiés.

Les attestations que les fournisseurs remettent au Canada peuvent être vérifiées à tout moment par ce dernier. Le Canada déclarera une réponse non recevable ou un manquement de la part de l'entrepreneur s'il est établi que le Répondant a, sciemment ou non, produit une fausse attestation pendant la période de qualification ou pendant la durée de tout arrangement en matière d'approvisionnement découlant de cette invitation à se qualifier et de tout contrat subséquent.

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

5.1 Attestations exigées avec la réponse

Les Répondants doivent fournir les attestations suivantes dûment remplies avec leur réponse.

5.1.1 Attestation de l'éditeur de logiciel-service

Les Répondants doivent inclure le Formulaire 3 – Attestation de l'éditeur de logiciel-service (SaaS) dans le cadre de la réponse.

5.1.2 Autorisation du fournisseur de services d'infonuagique du gouvernement du Canada

Les Répondants doivent inclure le Formulaire 4 – Autorisation du fournisseur de services d'infonuagique du gouvernement du Canada dans le cadre de la réponse.

5.1.3 Dispositions relatives à l'intégrité - Déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des instructions uniformisées, tous les Répondants doivent présenter avec leur réponse, **s'il y a lieu**, le formulaire de déclaration d'intégrité disponible sur le site Web Intégrité – Formulaire de déclaration (https://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html). Si le Canada détermine que les renseignements exigés dans le formulaire sont incomplets ou doivent être corrigés, le Canada donnera au répondant la possibilité de fournir les renseignements supplémentaires ou d'apporter la correction. Il est obligatoire de fournir les informations sur demande et comme demandé pendant la période d'évaluation.

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ

Un répondant provisoirement qualifié sera autorisé à participer au EAB.

Le Répondant provisoirement qualifié doit soumettre ses soumissions PCIE et ISCA à temps conformément aux modalités de la présente ISQ, avant l'expiration d'une période de trois semaines à compter de la date du courriel envoyé par TPSGC au Répondant provisoirement qualifié pour que leur soumission respective demeure recevable.

Un Candidat provisoirement qualifié qui échoue à son évaluation préliminaire ICA ou à son évaluation PCIE ne pourra pas continuer à participer à la phase EAB ou aux étapes suivantes de cet approvisionnement.

6.1 Participation, contrôle et influence étrangers (ISQ)

6.1.1 Un Répondant provisoirement qualifié qui, après vérification par le Canada, satisfait aux critères d'évaluation, aux exigences ainsi qu'aux autres modalités énoncées dans l'ISQ et qui en a été avisé par le Canada doit présenter une trousse complète de PCIE, y compris la documentation connexe, comme il est exigé dans les lignes directrices et le questionnaire relatifs à la PCIE, dans les trois semaines suivant la date du courriel envoyé directement au Répondant provisoirement qualifié par le bureau de la PCIE du Programme de sécurité des contrats (PSC) de TPSGC. Les directives et le questionnaire de la PCIE seront fournis dans ce courriel.

6.1.2 À tout moment au cours de l'évaluation de la PCIE, le Canada peut, à sa seule discrétion, demander des renseignements supplémentaires, des documents ou des éclaircissements au Répondant provisoirement qualifié. Le Canada peut en outre, à sa seule discrétion, exprimer ses préoccupations en matière de la PCIE au sujet du Répondant provisoirement qualifié et peut, mais n'est pas obligé, d'entamer des négociations sur d'éventuelles mesures d'atténuation avec le Répondant provisoirement qualifié pendant ou après l'évaluation de la PCIE. Toutes les communications entre le Canada et le Répondant provisoirement qualifié doivent rester confidentielles. Le Canada peut, à sa seule discrétion, disqualifier le Répondant provisoirement qualifié pour tout manquement à la confidentialité en plus de rechercher tout autre recours applicable comme des injonctions ou des dommages-intérêts.

6.1.3 Le Canada se réserve le droit d'utiliser toute information en sa possession pour l'évaluation de la PCIE. L'évaluation de la PCIE par le Canada donnera lieu à trois décisions possibles: «Sans la PCIE», «Avec PCIE; sans mesures d'atténuation requises» ou «Avec PCIE; mesures d'atténuation requises».

6.1.4 L'évaluation de la participation, du contrôle et de l'influence de l'étranger (PCIE) qui apporte des preuves de PCIE nécessitant des mesures d'atténuation sera examinée et approuvée par les autorités compétentes. Toute mesure d'atténuation approuvée doit rester en vigueur pendant toute la durée du processus d'approvisionnement. Si le Canada détermine que les mesures d'atténuation ne peuvent pas être mises en œuvre, il se réserve le droit de disqualifier le Répondant provisoirement qualifié et de l'empêcher participer aux étapes suivantes de l'approvisionnement y compris l'EAB.

6.1.5 Le Répondant provisoirement qualifié doit maintenir son statut PCIE « Sans PCIE » ou « Avec PCIE; mesures d'atténuation requises » pendant toute la durée du processus d'approvisionnement y compris durant le contrat. Le Répondant provisoirement qualifié doit immédiatement fournir au bureau de la PCIE la documentation relative à tout changement apporté à la structure organisationnelle ou de propriété de l'organisation et à toute augmentation

des revenus étrangers ou de la dette extérieure par rapport à ce qui a été déclaré au bureau de la PCIE dans l'évaluation initiale de la PCIE. Le Répondant provisoirement qualifié fera l'objet d'une nouvelle évaluation de la PCIE sur la base de ces nouvelles informations et des informations en possession du Canada le cas échéant, afin de déterminer à nouveau le statut PCIE.

6.1.6 Si le Répondant provisoirement qualifié reçoit une lettre de décision « Avec PCIE » ne pouvant pas comprendre de mesures d'atténuation, il ne sera pas en mesure d'obtenir les attestations de sécurité requises, d'obtenir et de maintenir une vérification d'organisation désignée (VOD) et les attestations de sécurité du personnel auprès du PSC. Par conséquent, il ne satisfera plus aux exigences relatives à la sécurité et sera jugé disqualifié du processus.

6.2 Exigence de sécurité prévue pour la PCIE - Étape de soumission:

6.2.1 Le processus suivant décrit est fourni à titre informatif seulement, en tant qu'exigence de sécurité PCIE anticipée. Le Canada se réserve le droit d'apporter toute modification aux processus prévus, y compris, mais sans s'y limiter, la suppression ou l'insertion d'un nouveau.

6.2.2 Avant d'avoir accès à des renseignements ou à des biens, le soumissionnaire ou l'entrepreneur retenu doit disposer d'une lettre de décision, qui se rapporte au présent contrat, qui expire à la fin dudit contrat ou des périodes de prolongation, et qui est émise par le bureau de la PCIE pour indiquer les résultats de l'évaluation de la PCIE. Cette évaluation sera menée sur le soumissionnaire ou l'entrepreneur retenu ainsi que sur les fournisseurs, sous-traitants pour ce contrat du soumissionnaire retenu.

6.2.3 Si la lettre de décision « Avec PCIE; mesures d'atténuation requises » demande de mettre en œuvre des mesures d'atténuation, celles-ci doivent être mises en œuvre et approuvées par le bureau de la PCIE avant que le soumissionnaire ou l'entrepreneur retenu ou son personnel ait accès à des renseignements ou à des biens. Ces mesures d'atténuation doivent rester en place pendant toute la durée du contrat, y compris les périodes de prolongation, le cas échéant.

6.2.4 Le PSC se réserve le droit de suspendre l'attestation de sécurité de l'organisation du soumissionnaire ou de l'entrepreneur retenu s'il est visé par une décision « Avec PCIE; mesures d'atténuation requises » et qu'il décide de ne pas mettre en œuvre les mesures d'atténuation requises.

6.2.5 Le soumissionnaire ou l'entrepreneur retenu doit maintenir son statut PCIE « Sans PCIE » ou « Avec PCIE; mesures d'atténuation requises » pendant toute la durée du contrat, y compris les périodes de prolongation, le cas échéant.

6.2.6 Le soumissionnaire ou l'entrepreneur retenu doit immédiatement fournir au bureau de la PCIE la documentation relative à tout changement apporté à la structure organisationnelle ou de propriété de l'organisation et à toute augmentation des revenus étrangers ou de la dette extérieure par rapport à ce qui a été déclaré au bureau de la PCIE dans l'évaluation initiale de la PCIE. Le soumissionnaire ou l'entrepreneur retenu fera l'objet d'une nouvelle évaluation de la PCIE en fonction de ces nouveaux renseignements dans le but de décider à nouveau du statut PCIE du soumissionnaire ou de l'entrepreneur retenu.

6.2.7 Si l'entrepreneur ou le soumissionnaire retenu reçoit une lettre de décision « Avec PCIE » et qu'il est impossible de mettre en œuvre les mesures d'atténuation, il ne sera pas en mesure d'obtenir les attestations de sécurité requises, d'obtenir et de maintenir une attestation de vérification d'organisation désignée (VOD) et les attestations de sécurité du personnel auprès du Programme

de sécurité des contrats (PSC). Par conséquent, il ne satisfera plus aux exigences relatives à la sécurité du contrat.

6.3 Renseignements généraux – Exigences relatives à la sécurité

Une version préliminaire de la liste de vérification des exigences en matière de sécurité (LVERS), y compris le guide de sécurité de la LVERS, a été incluse dans l'annexe C de la présente ISQ et les exigences prévues en matière d'attestation de sécurité sont décrites ci-dessous. Ces exigences sont fournies à titre informatif seulement et elles pourraient être modifiées. Ce processus s'ajoutera aux évaluations PCIE et ICA. Cependant, nous recommandons aux Répondants ne détenant pas les attestations de sécurité décrites dans la version provisoire de la LVERS d'entamer le processus pour obtenir ces attestations, afin de s'assurer de répondre aux exigences connexes. Les Répondants qualifiés qui ont besoin d'un parrainage de sécurité doivent en informer l'autorité contractante par écrit. La décision de retarder l'attribution du contrat afin de permettre au soumissionnaire retenu d'obtenir l'attestation de sécurité requise, demeure à l'entière discrétion de l'autorité contractante. Pour obtenir de plus amples renseignements sur les enquêtes de sécurité sur le personnel et les organismes, les Répondants devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada, à l'adresse suivante : http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html.

6.3.1 Clauses de sécurité anticipées pour les fournisseurs Canadiens – Étape de soumission

6.3.1.1 L'entrepreneur ou l'offrant doit, en tout temps pendant la durée du contrat ou de l'offre à commande, détenir une vérification d'organisation désignée (VOD) valide ainsi qu'une cote de protection et de production des documents de niveau **PROTÉGÉ B**, émise par le Programme de sécurité des contrats (PSC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

6.3.1.2 Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements, à des biens **PROTÉGÉS** ou à des lieux de travail dont l'accès est réglementé **doivent être citoyens ou résidents permanents du Canada ou citoyens des États-Unis d'Amérique, de la Nouvelle-Zélande, du Royaume-Uni ou de l'Australie et CHACUN doit** détenir une cote de fiabilité ou de sécurité valide de niveau **APPROFONDI ou SECRET, au besoin, et tous les autres doivent détenir une AUTORISATION D'ACCÈS AU SITE valide, au besoin,** délivrée ou approuvée par le PSC de TPSGC. Tant que les autorisations de sécurité des membres du personnel de l'entrepreneur requises aux termes du présent contrat n'ont pas été délivrées ou approuvées par le PSC de TPSGC, l'entrepreneur/les membres du personnel **NE PEUVENT PAS AVOIR ACCÈS** aux renseignements ou aux biens **PROTÉGÉS** et **ne peuvent pas entrer** sans escorte **dans les lieux** où de tels renseignements ou biens sont entreposés

6.3.1.3 L'entrepreneur **NE DOIT PAS** utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau PROTÉGÉ tant que le PSC de TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée ou approuvée, ces tâches pourront être exécutées au niveau **PROTÉGÉ B** (y compris un lien électronique au niveau **PROTÉGÉ B**).

6.3.1.4 L'entrepreneur ou l'offrant principal peut sous-traiter ou recourir à des tiers dans le cadre de l'exécution des travaux, pourvu que a) l'entrepreneur obtienne le consentement préalable écrit de l'autorité contractante, b) le PSC de TPSGC donne la permission écrite, c) le sous-traitant ou fournisseur tiers accepte de se conformer aux modalités du présent contrat et du contrat en sous-traitance, d) l'entrepreneur demeure responsable envers le Canada pour tous les travaux effectués par le sous-traitant ou le sous-traitant tiers ou l'offrant.

6.3.1.5 Tout entrepreneur ou offrant ou sous-traitant tiers qui offre des services d'infonuagique doit être approuvé par le gouvernement du Canada et respecter les exigences en matière de sécurité mentionnées dans le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage pour les renseignements classés « Protégé B/Intégrité moyenne/Disponibilité moyenne (PBMM) » pour la portée du logiciel-service disponible sur le marché proposé fourni. La conformité sera validée et vérifiée par l'entremise du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100) du Centre canadien pour la cybersécurité (CCC) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur qui a participé au processus doit fournir des documents confirmant qu'il a terminé le processus d'intégration avec i) une copie du rapport d'évaluation le plus récent fourni par le CCC; et ii) une copie du rapport sommaire le plus récent fourni par le CCC. Cela pourrait accélérer le processus de qualification.

L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :

a) Liste de vérification des exigences relatives à la sécurité et Guide de sécurité (s'il y a lieu), joints à l'annexe _____;
b) *Manuel de la sécurité des contrats* (dernière édition)

REMARQUE : Il y a plusieurs niveaux d'enquête de sécurité sur le personnel liés à ce dossier. Dans le cas présent, un guide de classification de sécurité doit être ajouté à la LVERS afin de clarifier ces niveaux de filtrage de sécurité. Le Guide de classification de sécurité est normalement rédigé par le chargé de projet ou le responsable de la sécurité de l'organisation.

6.3.2 Clauses de sécurité anticipées pour les fournisseurs étrangers – Étape de soumission

6.3.2.1 L'administration désignée en matière de sécurité (ADS canadienne) est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Services publics et Approvisionnement Canada (SPAC). L'ADS canadienne est chargée d'évaluer la conformité **des entrepreneurs et des sous-traitants** aux exigences relatives à la sécurité pour les entrepreneurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux entrepreneurs et aux sous-traitants destinataires étrangers constitués en société ou autorisés à faire des affaires dans un État autre que le Canada et qui livrent et exécutent à l'extérieur du Canada les services ou les travaux décrits dans l'énoncé des travaux, en plus des exigences en matière de sécurité et de protection des renseignements personnels.

6.3.2.2 **L'entrepreneur ou le sous-traitan**t étranger destinataire atteste que la prestation et l'approvisionnement du service géré et des opérations du Système de gestion de preuves numériques (SGPN) dans un modèle SaaS, y compris la surveillance et le soutien, seront fournis à partir du Canada ou de l'un des pays membres de la Five Eyes Intelligence Alliance (FVEY), soit l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis. De plus, **l'entrepreneur ou le sous-traitant** étranger destinataire atteste que la livraison et l'approvisionnement des dispositifs et des services de caméras corporelles, y compris le soutien, seront fournis à partir du Canada ou de l'un des pays membres de la Five Eyes

Intelligence Alliance (FVEY), notamment l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

6.3.2.3 **L'entrepreneur ou le sous-traitant** étranger destinataire doit en tout temps, au cours de la durée **du contrat ou du contrat de sous-traitance**, être inscrit auprès de l'autorité de surveillance compétente, administrée par le gouvernement, responsable de la protection des renseignements de niveau PROTÉGÉ AU CANADA et des renseignements personnels dans le ou les pays dans lesquels il est constitué en société ou exerce ses activités et est autorisé à faire des affaires et à traiter des renseignements de niveau PROTÉGÉ AU CANADA et des renseignements personnels. Il doit fournir à l'autorité contractante et à l'ADS canadienne la preuve de son inscription auprès de l'autorité de surveillance compétente, et le nom de l'autorité nationale responsable de la protection des renseignements personnels et de la sécurité.

6.3.2.4 L'entrepreneur ou le sous-traitant étranger destinataire doit soumettre, à la demande du Canada, le questionnaire sur la participation, le contrôle et l'influence étrangers (PCIE) y compris la documentation connexe, comme prescrit dans les lignes directrices et le questionnaire sur la PCIE, avant la date d'échéance indiquée dans le courriel envoyé par l'ADS canadienne.

6.3.2.5 Le Canada se réserve le droit de suspendre l'accès de l'entrepreneur ou du sous-traitant étranger destinataire à des renseignements de niveau PROTÉGÉ AU CANADA en fonction des renseignements inclus dans le dossier d'évaluation de la PCIE qu'il a fournis. Le Canada se réserve le droit de demander à l'entrepreneur ou au sous-traitant étranger destinataire de prendre des mesures de sécurité supplémentaires afin d'atténuer le risque de PCIE.

6.3.2.6 L'entrepreneur ou le sous-traitant étranger destinataire doit immédiatement fournir à l'ADS canadienne la documentation relative à tout changement apporté à la structure organisationnelle ou de propriété de l'organisation et à toute augmentation des revenus étrangers ou de la dette extérieure par rapport à ce qui a été déclaré au bureau de la PCIE dans l'évaluation initiale de la PCIE. Il fera l'objet d'une nouvelle évaluation de la PCIE en fonction de ces nouveaux renseignements dans le but de décider à nouveau de son statut de PCIE.

6.3.2.7 Le refus de l'accès aux renseignements de niveau PROTÉGÉ AU CANADA par l'ADS canadienne aura pour conséquence que l'entrepreneur ou le sous-traitant bénéficiaire étranger ne sera pas en mesure d'obtenir les cotes de sécurité nécessaires et, par conséquent, ne répondra pas aux exigences relatives à la sécurité prévues au contrat.

6.3.2.8 **L'entrepreneur ou le sous-traitant** étranger destinataire doit en permanence, pendant l'exécution **du contrat ou du contrat de sous-traitance**, remplir les exigences suivantes :

i. **L'entrepreneur ou le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.

ii. **L'entrepreneur ou le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services, ni assurer toute autre prestation tant que l'ADS canadienne n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le contrat. L'ADS canadienne fournira, par écrit, **à**

l'entrepreneur ou au sous-traitant étranger destinataire un formulaire d'attestation qui confirmera la conformité et l'autorisation de fournir les services prévus.

iii. **L'entrepreneur ou le sous-traitant** étranger destinataire doit désigner un agent de sécurité des contrats (ASC) autorisé qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera désignée par le président-directeur général ou le délégué officiel de **l'entrepreneur ou du sous-traitant** étranger destinataire soumissionnaire.

iv. **L'entrepreneur ou le sous-traitant** étranger destinataire doit nommer quelqu'un comme agent de protection de la vie privée, qui agira en tant que son représentant pour toutes les questions touchant aux renseignements personnels et aux dossiers. Cette personne sera désignée par le président-directeur général ou le délégué officiel de l'entrepreneur ou du sous-traitant étranger destinataire soumissionnaire.

v. **L'entrepreneur ou le sous-traitant** étranger destinataire n'autorisera pas l'accès à des renseignements ou à des biens de niveau **PROTÉGÉ AU CANADA**, sauf à son personnel, sous réserve des conditions suivantes :

a. le personnel a un besoin de savoir pour l'exécution du **contrat ou du contrat de sous-traitance**;

b. les membres du personnel ont fait l'objet d'une vérification du casier judiciaire valide, avec des résultats favorables, d'une agence gouvernementale reconnue ou d'une organisation du secteur privé dans **leur pays**, ainsi qu'une vérification d'antécédents, validée par l'ADS canadienne;

c. **l'entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que le personnel consente à la divulgation du casier judiciaire et des antécédents à l'ADS canadien et d'autres fonctionnaires du gouvernement canadien, sur demande;

d. l'entrepreneur ou le sous-traitant étranger destinataire qui doute que l'un de ses employés ait la capacité de consentir à la divulgation et à l'utilisation de ses renseignements personnels doit demander l'approbation de l'ADS canadienne (en collaboration avec l'autorité contractante) pour divulguer des renseignements **PROTÉGÉS AU CANADA** à cette personne;

e. le Gouvernement du Canada se réserve le droit de refuser l'accès aux renseignements ou aux biens de niveau **PROTÉGÉ AU CANADA à l'entrepreneur ou au sous-traitant** étranger et leur personnel destinataire pour un motif valable.

6.3.2.9 En outre, les membres du personnel de **l'entrepreneur ou du sous-traitant** étranger destinataire qui doivent avoir accès à des renseignements PROTÉGÉS avec des droits administratifs doivent TOUS détenir une cote de sécurité personnelle valide au niveau SECRET, comme l'exige le guide de classification de sécurité, accordée et approuvée par l'autorité de sécurité nationale (ASN) ou l'autorité désignée en matière de sécurité (ADS) de leur pays.

6.3.2.10 Les renseignements personnels et les biens **DE NIVEAU PROTÉGÉ AU CANADA** qui sont fournis **à l'entrepreneur ou au sous-traitant** étranger destinataire, ou qui sont produits par **ce dernier**, doivent respecter les conditions suivantes :

a. ils ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise (ni à un représentant de cette autre personne ou de cette autre

entreprise) qui n'est pas directement lié à l'exécution **du contrat ou du contrat de sous-traitance** sans le consentement écrit préalable du gouvernement du Canada. Ce consentement doit être obtenu auprès de son autorité de protection des données (APD) et de l'autorité contractante (en collaboration avec l'ASD canadienne);

b. ils ne doivent pas servir à d'autres fins que l'exécution **du contrat ou du contrat de sous-traitance** sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de son autorité de protection des données (APD)/ADS en collaboration avec l'ADS canadienne.

6.3.2.11 **L'entrepreneur ou le sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements ou de biens **PROTÉGÉS AU CANADA** hors des établissements de travail visés; et **l'entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

6.3.2.12 **L'entrepreneur ou le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements ni les biens **PROTÉGÉS AU CANADA** pour répondre à des besoins autres que l'exécution **du contrat ou du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette approbation doit être obtenue auprès de l'ADS canadienne.

6.3.2.13 **L'entrepreneur ou le sous-traitant** étranger destinataire doit détenir en permanence, pendant l'exécution **du contrat ou du contrat de sous-traitance**, une autorisation de détenir des renseignements (ADR) approuvée de niveau **PROTÉGÉ B AU CANADA**.

6.3.2.14 Tous les renseignements et les biens **PROTÉGÉS AU CANADA**, fournis **à l'entrepreneur ou au sous-traitant** étranger destinataire ou produits par lui, doivent également être protégés comme suit :

a. **L'entrepreneur ou le sous-traitant** étranger destinataire devra signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou a lieu de croire que des renseignements ou des biens **PROTÉGÉS AU CANADA** relatifs à l'exécution **du contrat ou contrat de sous-traitance** ont été compromis.

OU

a. **L'entrepreneur ou le sous-traitant** étranger destinataire doit signaler immédiatement à son ADS/autorité de protection des données nationale et à l'ADS canadienne (en collaboration avec l'autorité contractante) tous les cas dans lesquels il sait ou a lieu de croire que des renseignements personnels fournis ou générés, conformément au présent **contrat ou contrat de sous-traitance**, ont été perdus, ou ont été utilisés ou divulgués en contrevenant aux présentes exigences en matière de sécurité.

b. L'entrepreneur ou le sous-traitant étranger destinataire doit contrôler l'accès à toutes les bases de données dans lesquelles sont stockées des données liées au présent contrat ou au contrat de sous-traitance, afin que seules les personnes titulaires de la cote de sécurité appropriée puissent avoir accès à la base de données, soit au moyen d'un mot de passe ou d'un autre moyen d'accès (comme des mesures de contrôle biométrique).

c. L'entrepreneur ou le sous-traitant étranger destinataire doit s'assurer que toutes les bases de données comprenant des données relatives au présent contrat ou au contrat de sous-traitance et archivées sont isolées sur les plans physique et logique, en d'autres termes qu'elles n'ont aucune connexion directe ou indirecte de quelque type que ce soit avec d'autres bases de données.

d. **L'entrepreneur ou le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements ou les biens **PROTÉGÉS AU CANADA** à un autre gouvernement, ni à une autre personne physique ou morale, ni à leurs représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu auprès de l'ADS canadienne.

e. **L'entrepreneur ou le sous-traitant** étranger destinataire doit assurer une protection des renseignements et des biens **PROTÉGÉS AU CANADA** aussi stricte que celle assurée par le gouvernement du Canada, conformément aux politiques nationales ainsi qu'aux lois et règlements en matière de sécurité nationale, et dans le respect des prescriptions prévues par l'ADS canadienne.

f. L'entrepreneur ou le sous-traitant étranger destinataire doit marquer tous les renseignements et biens PROTÉGÉS AU CANADA que le gouvernement du Canada lui fournit en vertu du présent contrat ou contrat de sous-traitance de la classification de sécurité équivalente utilisée par son pays et conformément aux lois, aux règlements et aux politiques de son pays et à l'entente de sécurité bilatérale internationale concernant la sécurité industrielle conclue avec le Canada.

g. À la fin des travaux, **l'entrepreneur ou le sous-traitant** étranger destinataire doit remettre au gouvernement du Canada tous les renseignements et biens **PROTÉGÉS AU CANADA** fournis ou produits en vertu **du contrat ou du contrat de sous-traitance**, y compris tous les renseignements et biens **PROTÉGÉS AU CANADA** remis à ses sous-traitants ou produits par eux.

h. **L'entrepreneur ou le sous-traitant** étranger destinataire qui doit accéder à des renseignements personnels ou à des biens de niveau **PROTÉGÉ AU CANADA** ou à des sites à accès restreint au Canada en vertu du présent contrat doit soumettre une demande d'accès au site à l'agent de sécurité ministériel de la **Gendarmerie royale du Canada**.

i. **L'entrepreneur ou le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique (et transférer au moyen d'un lien électronique) des renseignements de niveau **PROTÉGÉ AU CANADA** avant que l'ADS canadienne lui en donne le droit.

j. **L'entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données y compris les bases de données de sauvegarde utilisées par les organisations pour offrir les services décrits dans le Système de gestion de preuves numériques (SGPN) dans un modèle SaaS proposées qui renferment des renseignements de niveau **PROTÉGÉ AU CANADA** relativement aux travaux se trouvent au Canada.

6.3.2.15 Le Canada peut vérifier en tout temps la conformité **de l'entrepreneur ou du sous-traitant** étranger destinataire avec ces exigences relatives à la sécurité supplémentaires prévues au contrat. À la demande de l'autorité contractante, **l'entrepreneur ou le sous-traitant** étranger destinataire doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux ainsi qu'aux renseignements personnels et dossiers de niveau **PROTÉGÉ AU**

CANADA en tout temps jugé raisonnable. Si le Canada découvre un problème durant la vérification, **l'entrepreneur ou le sous-traitant** étranger destinataire doit le corriger immédiatement à ses frais.

6.3.2.16 Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne.

6.3.2.17 Tous les contrats de sous-traitance attribués à un entrepreneur étranger destinataire ne doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

6.3.2.18 Tous les contrats de sous-traitance attribués par un tiers étranger destinataire NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

6.3.2.19 Tout tiers fournisseur qui devra avoir accès à des renseignements PROTÉGÉS AU CANADA dans le cadre du présent contrat doit se conformer à toutes les exigences relatives à la sécurité prévues au présent contrat.

6.3.2.20 Le Canada a le droit de rejeter toute demande visant l'accès électronique aux renseignements de niveau PROTÉGÉ AU CANADA liés aux travaux dans un autre pays ainsi que le traitement, la production, la transmission ou l'entreposage de ces renseignements s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

6.3.2.21 **L'entrepreneur ou le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'annexe C.

6.4 Évaluation de l'intégrité de la chaîne d'approvisionnement (ICA)

6.4.1 Afin d'être pleinement qualifié, un Répondant provisoirement qualifié doit, réussir un processus d'évaluation préliminaire de l'intégrité de la chaîne d'approvisionnement (ICA).

6.4.2 Une évaluation supplémentaire, plus détaillée et complète de l'intégrité de la chaîne d'approvisionnement (ICA) sera effectuée au stade de la demande de propositions. L'ICA préliminaire sera évaluée sur la base des informations fournies dans le **formulaire 5 - Informations sur la sécurité de la chaîne d'approvisionnement (ISCA)** par le répondant (voir ci-joint) ainsi que les pièces justificatives demandées par le Canada et fournies par le répondant provisoirement qualifié. Le but de ces évaluations ICA est de s'assurer que tous les sous-

traitants, produits, équipements, logiciels, micrologiciels et services qui sont achetés par le Canada satisfont aux normes de sécurité et de chaîne d'approvisionnement.

6.4.3 L'évaluation préliminaire de l'ICA est obligatoire à l'étape de l'ISQ. L'annexe D, Évaluation préliminaire de l'intégrité de la chaîne d'approvisionnement, décrit le processus plus en détail, y compris les renseignements à soumettre. L'ICA est une importante exigence ministérielle. Confronté à des cybermenaces de plus en plus complexes, le Canada s'engage à inclure des processus d'évaluation de la sécurité améliorés dans l'ISQ, la DP et le contrat subséquent.

6.4.4 Le Répondant provisoirement qualifié doit fournir les informations décrites à l'Annexe D - Sécurité de la chaîne d'approvisionnement Processus d'évaluation de l'information dans le cadre de l'évaluation préliminaire de l'ICA. Le Répondant provisoirement qualifié n'est pas tenu de remplir toutes les sections du Formulaire 5 - Informations sur la sécurité de la chaîne d'approvisionnement, mais seulement celles exigées par l'Annexe D. Les Répondants qualifiés seront tenus de fournir l'ensemble des informations sur la sécurité de la chaîne d'approvisionnement au moment de la DDP.

ANNEXE A

APERÇU ET DESCRIPTION DE HAUT NIVEAU DU BESOIN
CAMÉRAS CORPORELLES ET SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES

L'aperçu suivant des besoins anticipés est fourni à titre indicatif à ce stade uniquement. Cette annexe met en évidence certaines des exigences prévues qui pourraient devoir être prises en considération à la fois pour la DDP et le contrat subséquent. Veuillez noter que les exigences prévues suivantes sont sujettes à changement, peuvent ne pas être complètes et l'énoncé complet des exigences sera publié à l'étape de la demande de propositions.

1. Contexte

1.1 La Gendarmerie royale du Canada (GRC) est le service de police national du Canada et a comme mandat de maintenir l'ordre dans l'ensemble du pays, à l'échelle communautaire, municipale, provinciale, territoriale et fédérale. La GRC fournit des services de police fédéraux, provinciaux, territoriaux et municipaux aux Canadiens dans 10 provinces, 3 territoires, 150 municipalités et plus de 600 collectivités autochtones, ce qui comprend la prestation de services de police fédéraux et de services de police spécialisés à l'appui de centaines d'autres services de police et organismes de sécurité publique partout au Canada.

1.2 La GRC est une organisation de 5 milliards de dollars qui compte environ 30 000 employés, dont 19 000 policiers. La GRC possède plus de 1,3 milliard de dollars en actifs, dont 3 362 immeubles et 14 749 véhicules partout au pays. La GRC a décidé de faire des caméras corporelles et d'un système de gestion des preuves numériques (SGPN) une norme nationale pour tous les agents de police de première ligne et de service général au pays, ce qui représente entre 10 000 et 15 000 agents. Bon nombre de ces policiers travaillent dans des régions rurales et éloignées dans environ 750 détachements à travers le Canada.

2. Portée

2.1 La GRC s'est engagée à faire en sorte que les Canadiens se sentent protégés par leur service de police national et aient confiance en lui. Le Canada cherche à attribuer un contrat à un entrepreneur qui fournira une solution qui inclut des caméras corporelles et un logiciel-service national de gestion des preuves numériques en tant que service entièrement géré (ci-après appelé « service ou services »). Il est prévu que, en plus de la GRC, d'autres ministères, organismes ou sociétés d'État fédéraux et des administrations provinciales, territoriales et municipales pourraient utiliser le contrat subséquent pour accéder aux services.

3. Principal motif de changement

3.1 Le public surveille plus attentivement que jamais les interactions de la police (entre autres la GRC) avec la population. Une des principales initiatives favorisant la transparence et la responsabilité est le déploiement national de caméra corporelle pour les policiers de la GRC.

Bien qu'elle ne représente pas une panacée, l'utilisation des caméras corporelles dans d'autres corps policiers autour du globe a permis d'accroître la transparence, tout en réduisant le temps nécessaire pour régler les plaintes.

4. Utilisation de caméra corporelle

4.1 Depuis 15 ans, les caméras corporelles ont été mises en place partout dans le monde. Au Canada, des caméras corporelles sont désormais utilisées – ou sont en voie de l'être – par de nombreux services de police d'envergure, notamment à Calgary, à Halifax, à Toronto et à Peel.

4.2 La GRC étudie la technologie des caméras corporelles depuis plusieurs années. Elle en a d'ailleurs fait l'essai dans le cadre de projets pilotes. En 2017, la GRC a distribué douze caméras corporelles à ses membres de Happy Valley-Goose Bay et de Cartwright, à Terre-Neuve-et-Labrador (Division B), comme déploiement limité et temporaire d'équipement afin de soutenir les opérations policières. Ainsi, la GRC a pu évaluer la fonctionnalité de ces appareils dans un contexte opérationnel.

4.3 Après avoir consulté les membres de la communauté, les intervenants et les représentants des gouvernements fédéral et territorial, un projet pilote restreint a été lancé à Iqaluit à l'automne 2020 en vue de tester les procédures et les lignes directrices provisoires et de déterminer les ressources nécessaires pour soutenir le fonctionnement permanent des caméras et des preuves vidéo. L'information et les données recueillies dans le cadre de ce projet pilote serviront à améliorer la politique opérationnelle, les procédures et les programmes de formation à l'appui du programme national de caméra corporelle et de système de gestion des preuves numériques (SGPN) de la GRC.

4.4 Des projets pilotes ont déjà eu lieu, mais ceux-ci portaient surtout sur les fonctions et les limites des caméras, l'incidence de leur utilisation sur les opérations et les politiques qui régiront leur usage. La GRC a conservé un petit nombre de ces caméras pour une utilisation limitée lors d'événements majeurs.

5. Objectifs et résultats opérationnels

5.1 Le Canada cherche à obtenir les services d'un entrepreneur pour l'appuyer dans sa mise en œuvre nationale des caméras corporelles et d'un système de gestion des preuves numériques national, comme il est expliqué aux articles 6.4.1 et 6.4.2. La GRC prévoit avoir un entrepreneur en place d'ici l'automne 2021. Par la suite, les premières caméras seront distribuées de manière progressive, aboutissant à une mise en œuvre à l'échelle nationale avec un déploiement complet, qui comprendra un SGPN robuste et une formation connexe, dans un délai de 12 à 18 mois.

5.2 Grâce à la mise en œuvre d'un programme national de caméra corporelle et de SGPN à la GRC, les Canadiennes et Canadiens peuvent s'attendre à ce qui suit :

- l'amélioration de la transparence et de la responsabilité de la police, ce qui renforcera la confiance du public envers la police;
- l'amélioration du caractère légitime et respectueux des interactions entre la population et la police;
- l'amélioration de la collecte de preuves et des poursuites judiciaires;
- le traitement accéléré des plaintes du public et le retrait d'un plus grand nombre de plaintes en raison des preuves vidéo.

5.3 Les améliorations les plus tangibles devraient être l'amélioration de la collecte de preuves, la réduction des délais de règlement des plaintes et l'augmentation de la transparence. Les

preuves vidéo fourniront un moyen indépendant et objectif d'enregistrer les incidents et les interactions entre les policiers et la population.

6. Portée fonctionnelle

6.1 L'entrepreneur retenu devra fournir un service entièrement géré qui appuiera le déploiement des caméras corporelles et de l'équipement connexe ainsi que la gestion continue du cycle de vie du matériel, y compris le remplacement, l'entretien et la réparation. L'entrepreneur fournira également des services à l'appui de la mise en œuvre d'un SGPN logiciel-service (SaaS) ainsi que tout autre service requis pour appuyer les activités continues du programme des caméras corporelles et du SGPN de la GRC.

6.2 Ce service devra être adaptable pour répondre aux exigences de la GRC, y compris celles des régions urbaines, rurales et éloignées de la GRC, et être en mesure d'offrir des capacités dans plusieurs territoires de compétence. Le Service doit être évolutif, de façon à doter entre 10 000 et 15 000 policiers de la GRC de caméra corporelle et d'un SGPN ainsi que d'autres utilisateurs du SGPN à l'échelle de la GRC.

6.3 L'entrepreneur devra tenir compte de défis tels que la saisie et le stockage de preuves numériques dans des zones où la bande passante des données est limitée, la capacité des caméras corporelles de fonctionner dans une vaste gamme de températures compte tenu des divers emplacements et l'activation et la saisie automatisée de preuves numériques dans des situations d'urgence et de stress élevé.

6.4 L'entrepreneur devra livrer les éléments suivants à l'appui du programme national de caméra corporelle et de SGPN de la GRC :

6.4.1 Caméras corporelles

L'entrepreneur fournira des caméras corporelles lui appartenant ainsi que l'équipement connexe. Parmi les services qui peuvent être requis, citons les suivants :

- provisionnement;
- distribution;
- soutien technique;
- formation;
- entretien, remplacement et réparation;
- élimination sécuritaire;
- renouvellement continu.

Voici quelques exemples d'équipement connexe :

- plusieurs options de fixation sur les uniformes;
- supports de fixation ou attaches;
- Les stations d'accueil et les câbles de recharge connexes;
- Divers mécanismes de déclenchement automatisés (p. ex. étui, arme à impulsions, voiture).

6.4.2 SGPN

L'entrepreneur fournira un SGPN qui servira de SGPN SaaS. Parmi les services qui peuvent être requis, citons les suivants :

- configuration, intégration et mise à l'essai;
- soutien technique;
- formation;

- mise en œuvre;
- déploiement;
- mise en place des services informatiques;
- opérations;
- entretien;
- renouvellement continu.

Parmi les capacités requises du SGPN, citons les suivantes :

- stockage sécurisé et fiable des données Protégé B;
- téléchargement des fichiers vidéo des caméras corporelles et d'autres fichiers multimédias (p. ex. vidéo, audio, photo, texte) provenant de diverses sources;
- recherche et récupération de preuves numériques;
- capacités d'intégration sous la forme d'une interface de programmation d'applications (API) sécurisée;
- gestion, retranchement et modification de l'information saisie;
- capacité de transmettre des éléments de preuve à l'interne comme à l'externe;
- migration des données.

7. Capacités fonctionnelles, résultats et valeur opérationnelle

Le tableau suivant présente les outils et les capacités opérationnelles que le Canada devra demander à l'entrepreneur d'examiner lorsqu'il proposera des solutions dans le cadre de cette initiative. La liste des capacités servira à établir la portée fonctionnelle et d'élaborer les exigences ministérielles et opérationnelles détaillées expliquées dans les étapes ultérieures du processus d'acquisition. Cette liste des outils et des capacités peut évoluer durant le processus d'acquisition.

Secteur fonctionnel	Capacité	Valeur opérationnelle
Caméras corporelles	• **Robuste et facile à utiliser**	• Des caméras pouvant résister aux demandes physiques du travail d'un policier sans compromettre la sécurité de ce dernier. • Capacité de l'activer avec une seule main et impossibilité de la désactiver accidentellement.
	• **Options flexibles et sécurisées de fixation sur les uniformes**	• Capacité de l'insérer dans l'espace disponible et de l'intégrer visuellement aux uniformes des agents. • Compatibilité avec plusieurs options de montage uniformes pouvant répondre à divers besoins opérationnels. • Capacité d'être bien attachée à l'uniforme des agents.
	• **Fonctionnement dans les régions éloignées et rurales**	• Des caméras pouvant résister à une vaste gamme de températures, de la chaleur des étés au froid extrême des hivers canadiens sans que son rendement soit affecté ou que sa capacité à enregistrer les preuves numériques soit compromise.
	• **Téléchargement automatisé des preuves numériques**	• Capacité d'automatiser le téléchargement des données des caméras corporelles dans le SGPN dans les régions urbaines, rurales et éloignées afin de réduire au minimum le travail supplémentaire des policiers à la fin de leur quart de travail. • Capacité de télécharger des éléments de preuves de la caméra corporelle vers le SGPN dans des endroits

		éloignés où la bande passante est limitée (p. ex. la caméra corporelle se branche directement au SGPN au moyen d'un réseau cellulaire).
	• **Autonomie de la pile et capacité de stockage**	• Durée de vie et capacité de stockage suffisantes pour s'assurer que l'agent de police est en mesure de saisir tous les enregistrements requis pendant toute la durée du quart de travail
	• **Gestion de l'équipement**	• Approvisionnement, distribution, entretien, réparation, remplacement, mise à niveau et élimination des caméras corporelles et de tout l'équipement connexe. • Disponibilité de fiches techniques complètes, de documents de spécifications, d'essais diagnostiques et de tout manuel de réparation sur le terrain pour le matériel de caméra corporelle, le micrologiciel des caméras corporelles et le matériel d'interface connexe (surtout s'il est exclusif) qui est utilisé par le service pour aider à extraire les données des caméras corporelles endommagées.
SGPN	• **Stockage en nuage des preuves numériques**	• Capacité de télécharger en toute sécurité des données numériques provenant des caméras corporelles et d'autres fichiers multimédias vers une solution de stockage infonuagique. • Fournir une solution qui fonctionne dans les régions rurales et éloignées où la bande passante est faible.
	• **Gestion des éléments de preuve**	• Permettre au Canada de stocker et d'organiser les supports numériques de manière à faciliter l'organisation et la récupération des données. De plus, il faut prendre en compte la mobilité des ressources de la GRC qui changent de détachement tout en restant au sein d'une même division ou qui passent parfois d'une division à l'autre. • Fournir un service dans les deux langues officielles, soit le français et l'anglais, qui répond aux normes sur l'accessibilité du gouvernement du Canada, tel que le définit le point 8.1.
	• **Retranchement et modification**	• Intégrer des outils sécurisés conviviaux qui permettent de retrancher des éléments et de modifier les enregistrements numériques en vue de leur divulgation. Les outils qui favorisent l'automatisation et réduisent le nombre d'interventions manuelles au moyen de caractéristiques d'automatisation des processus robotisés sont souhaitables.
	• **Divulgation**	• Permettre la divulgation sécuritaire des preuves à divers intervenants externes dans plusieurs territoires de compétence partout au pays.
	• **Communication d'information**	• Permettre différents types de communication (p. ex. information géographique, de localisation, organisationnelle, de la division). • Répondre à différents besoins en matière de communication d'information (p. ex. de nature administrative, vérification, rendement).

	• **Protection des renseignements personnels et sécurité**	• Respecter les dispositions législatives fédérales en matière de protection de la vie privée et les normes de sécurité et fournir des outils pour gérer et contrôler l'accès des utilisateurs. • Le service doit : a) satisfaire aux exigences de niveau de sécurité Protégé B du gouvernement du Canada (GC) b) être hébergé par un fournisseur « qualifié » de services d'infonuagique du GC conformément à l'article 8.3.2; c) satisfaire au profil des mesures de sécurité du GC pour les services de TI du GC fondés sur l'informatique en nuage résider sur des IaaS et PaaS conformes au profil des mesures de sécurité du GC pour les services fondés sur l'informatique en nuage du GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html).
	• **Interfaces et intégration**	• Les preuves numériques peuvent être intégrées aux données des systèmes sources de la GRC aux fins de gestion des dossiers opérationnels.
	• **Gestion de l'accès des utilisateurs**	• La GRC sera en mesure de déterminer des contrôles d'accès en fonction des rôles. • Capacité d'utiliser des identités fédérées pour la gestion de l'accès des utilisateurs.
Services interfonctionnels	• **Formation**	• Fournir du matériel et des services de formation pour appuyer la formation de tous les policiers de la GRC et des utilisateurs des caméras corporelles et du SGPN dans les deux langues officielles du Canada.
	• **Soutien technique**	• Soutien 24 heures sur 24, 7 jours sur 7 dans les deux langues officielles du Canada pour l'utilisation des caméras corporelles et du SGPN, qui répond aux normes de niveau de service du Canada.
	• **Signalement et résolution des pannes et des problèmes de rendement**	• Fournir un service qui surveille et signale les pannes ou les erreurs et proposer des solutions aux pannes et aux erreurs en tenant compte d'un ensemble de normes de service. • Les utilisateurs doivent avoir accès à des rapports sur différentes données liées au rendement et à l'utilisation des services.

	• **Disponibilité / continuité des activités**	• Les utilisateurs doivent pouvoir continuer d'enregistrer des événements durant une perturbation majeure (p. ex. panne de courant, interruption des télécommunications). • Les données inactives des utilisateurs doivent pouvoir être stockées et protégées, y compris les données sauvegardées ou conservées aux fins de redondance à l'intérieur des frontières géographiques du Canada.

8. Exigences obligatoires prévues

Il est prévu que toute future demande de soumissions comportera les exigences OBLIGATOIRES suivantes. Celles-ci ont trait à la capacité de l'entrepreneur d'élaborer et de déployer un service qui appuierait le programme de caméra corporelle et de SGPN de la GRC. La liste complète des exigences à satisfaire à l'appui du programme de caméra corporelle et de SGPN de la GRC est en cours d'élaboration et sera fournie aux étapes suivantes du processus d'approvisionnement.

8.1 Accessibilité

Le service de SGPN doit assurer la conformité de niveau AA aux Règles pour l'accessibilité des contenus Web (WCAG) 2.1 telles que décrites au lien suivant : https://www.w3.org/TR/WCAG21/

Les règles comprennent, entre autres, ce qui suit :

- Utilisation correcte du balisage sémantique/hiérarchique (essentiel pour les lecteurs d'écran) ;
- Texte optionnel pour toutes les images contenant de l'information (aucun texte pour les images décoratives) ;
- Possibilité pour les utilisateurs d'accéder à toutes les fonctionnalités au moyen de la touche de tabulation (fonctionnalité complète sans souris) ;
- Liens s'ouvrant dans la même fenêtre de navigateur (pas de nouvel onglet ni de nouvelle fenêtre) ;
- Tableaux conformes aux spécifications des WCAG.

Les installations et les points d'intérêt présentés visuellement sur une carte doivent aussi être présentés en format texte accessible.

Le service de SGPN doit être conforme à la *Norme sur l'accessibilité des sites Web* du gouvernement du Canada telle que décrite au lien suivant : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

8.2 Volet multimédia des services

8.2.1 Aperçu

Les volets de travail suivants constitueront les principales responsabilités de l'entrepreneur en ce qui concerne le démarrage, le déploiement et l'opérationnalisation du programme de caméra corporelle et de SGPN de la GRC :

- Planification de l'intégration
- Planification et mise en œuvre

- Formation et gestion du changement organisationnel
- Déploiement
- Phase de fonctionnement
- Innovation et amélioration des solutions
- Services de transition
- Services supplémentaires

Les articles ci-dessous donnent un aperçu des volets de travail.

D'autres descriptions, la portée, les rôles, les responsabilités, les renseignements sur l'état actuel et les exigences seront examinés et peaufinés avec les fournisseurs qualifiés de l'IQ au cours des étapes suivantes du processus d'approvisionnement.

8.2.2 **Planification de l'intégration**

L'entrepreneur doit fournir des services professionnels au Canada afin de déterminer la façon la plus appropriée de déployer les caméras corporelles et le SGPN à l'échelle nationale. Il incombera à l'entrepreneur de définir la ou les catégories de services professionnels qui conviennent le mieux à l'exécution de cette tâche. Ce travail comprend des considérations clés pour le déploiement afin d'assurer un succès optimal et le risque de gestion. Une telle planification devrait reposer sur une expérience de la gestion de déploiements de portée et d'échelle semblables à celles exigées par le Canada. La planification comprend un soutien pour définir le nombre de ressources canadiennes nécessaires à la réussite du processus d'intégration et le nombre de ressources requises sur une base permanente pour soutenir la gestion de l'équipement, la préparation et le montage de l'information numérique ainsi que la diffusion. Les livrables connexes seront définis plus précisément dans les demandes de soumissions qui en résulteront, s'il y a lieu.

8.2.3 **Planification et mise en œuvre**

L'entrepreneur doit fournir des services de mise en œuvre, y compris la planification et la gestion de projet, la conception de systèmes, de données et de processus, la mise en œuvre de solutions, la configuration, les liens avec les systèmes du Canada et la mise à l'essai et le déploiement. Cette tâche comprend également le soutien à la planification de la continuité des activités et à la planification de la reprise en cas de sinistre afin d'assurer le maintien des services pendant des perturbations (panne de courant, interruption des services de télécommunication, perte de la connexion Internet, panne ou interruption des principaux services, etc.).

8.2.4 **Soutien à la formation et à la gestion du changement organisationnel**

L'entrepreneur doit fournir l'expertise et les ressources nécessaires pour soutenir l'élaboration d'un plan de gestion du changement et de formation fondé sur l'expérience avec d'autres solutions d'envergure similaire. Cela comprend un aperçu des principales étapes que chaque division et chaque détachement devrait entreprendre pour se préparer à l'intégration ainsi que des listes de vérification ou une évaluation de l'état de préparation à effectuer avant l'intégration. L'entrepreneur sera tenu de contribuer à l'ébauche des politiques et procédures qui s'appliquent actuellement aux caméras corporelles et à la gestion des preuves numériques pour en assurer la conformité avec les pratiques exemplaires en vigueur dans le milieu, s'il y a lieu. De plus, l'entrepreneur fournira des outils et du matériel de formation pour la caméra corporelle et le SGPN qui pourront être intégrés aux programmes de formation générale à l'intention des policiers.

8.2.5 **Déploiement**

8.2.5.1 **Déploiement initial**

L'entrepreneur devra prendre en charge un déploiement initial de caméra corporelle dans un secteur rural, une région éloignée et un centre urbain. Il devra faire l'essai d'un certain nombre d'éléments, notamment les caméras corporelles, le système de gestion des preuves numériques (SGPN) et les politiques et les modalités sur l'utilisation des caméras corporelles et du SGPN. Il est également prévu que ce déploiement initial permettra la mise à l'essai des plans et des outils de formation et de gestion du changement organisationnel en cours d'élaboration.

8.2.5.2 **Ajustements fondés sur le déploiement initial**

Le gouvernement du Canada s'attend à effectuer une évaluation officielle du déploiement initial, et l'entrepreneur devra peut-être prendre en charge (ou faire) les mises à jour et les modifications au programme des caméras corporelles et du SGPN.

8.2.5.3 **Déploiement progressif**

L'entrepreneur doit gérer et prendre en charge le déploiement progressif des caméras corporelles et du SGPN partout au pays. L'entrepreneur sera tenu d'appuyer la planification de ce déploiement progressif et de fournir des conseils et une orientation sur la séquence et l'ampleur de chaque phase de déploiement en fonction des leçons tirées du déploiement initial.

8.2.5.4 **Phase d'exploitation**

L'entrepreneur doit assurer la gestion et le soutien des services après chaque phase du déploiement, ce qui comprend un ensemble de responsabilités décrites dans le contrat et un ensemble de normes de service également définies dans le contrat.

8.2.5.5 **Innovation et amélioration des services**

L'entrepreneur doit collaborer avec le Canada pour innover et améliorer les services qu'il fournit. Il peut s'agir notamment de proposer de nouvelles technologies ou de nouveaux processus pour améliorer l'utilisation par le gouvernement du Canada des caméras corporelles et du SGPN et d'en optimiser la capacité.

8.2.5.6 **Services de transition**

L'entrepreneur doit fournir un plan de transition de sortie qui décrit les activités et les processus requis en cas de résiliation d'une entente de produit SaaS (p. ex., l'entrepreneur fait faillite, la fin du contrat, etc.).

8.2.5.7 **Services supplémentaires**

On pourrait demander à l'entrepreneur de fournir des services supplémentaires pour appuyer le programme des caméras corporelles et du SGPN afin de répondre aux besoins changeants (p. ex. des services professionnels offerts en collaboration avec le gouvernement du Canada afin d'accepter d'autres types de preuves).

8.3 **Obligations en matière de sécurité**

Les domaines suivants constituent un sous-ensemble plus vaste d'exigences de sécurité qui sont en cours d'élaboration et ne constituent pas une liste exhaustive. Les données

organisationnelles sont définies comme toutes les données créées ou traitées par la GRC, ses organismes partenaires ou le gouvernement du Canada au sein du Service. Les données organisationnelles comprennent toutes les métadonnées et les registres dérivés ou liés aux données organisationnelles.

8.3.1 **Assurance d'une tierce partie : Certifications et rapports**

Au moment de la soumission, l'entrepreneur doit démontrer que les données organisationnelles, son infrastructure (y compris les services IaaS, PaaS ou SaaS où les données du Canada sont hébergées) et les points de prestation des services sont protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans ses pratiques et politiques de sécurité.

L'entrepreneur doit démontrer que les mesures prévues dans ses pratiques et politiques de sécurité sont conformes aux exigences énoncées dans les certifications et les rapports de vérification suivants en fournissant des rapports d'évaluation ou des certifications de tiers indépendants qui portent sur la couche de service SaaS de l'offre de services, en fournissant les deux (2) rapports de certification suivants :

a) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Certification obtenue par un organisme de certification accrédité; **ET**
b) Contrôles au niveau du système et au niveau organisationnel de l'AICPA (Service Organization Control) (SOC) 2 Type II Rapport de vérification 2 de type II se rapportant aux principes des services Trust (sécurité, disponibilité, intégrité du traitement et confidentialité) – produit par un comptable public accrédité (CPA) indépendant.

Autres certifications pouvant être examinées et/ou prises en compte :

a) ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services infonuagiques réalisés par un organisme de certification accrédité;
b) ISO/EIC 27018:2019 Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII; **ET**
c) Cloud Security Alliance (CSA), certification et attestation STAR de niveau 2 de la CSA.

Chaque rapport de certification ou de vérification fourni doit :

a) indiquer la raison sociale légale de l'entrepreneur ou du sous-traitant concerné;
b) indiquer la date de certification de l'entrepreneur ou du sous-traitant et l'état de cette certification;
c) indiquer les services compris dans le champ d'application du rapport de certification. Si des exclusions sont relevées, ou s'il est nécessaire de séparer une organisation de sous-services tels que l'hébergement de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être fourni.

Avant l'attribution du contrat, à la demande du gouvernement Canada, tous les rapports de vérification connexes doivent être accompagnés d'éléments de preuve à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité avec la certification ISO, et elles doivent clairement divulguer toutes les constatations importantes du vérificateur. Avant d'accepter la charge de travail de la GRC, l'entrepreneur doit régler les problèmes préoccupants pour le gouvernement du Canada à la satisfaction de celui-ci. Si l'entrepreneur n'est pas en

mesure de régler l'un des problèmes à la satisfaction du gouvernement du Canada, ce dernier aura le droit de résilier le contrat pour manquement et mis à la disposition du gouvernement.

Chaque rapport COS 2 type II doit avoir été réalisé dans les 12 mois précédant le début du contrat. Chaque rapport ISO 27001 doit avoir été réalisé dans les trois derniers mois avant le début du contrat. Une lettre d'intervalle peut être remise afin de démontrer que l'entrepreneur se trouve dans un processus de renouvellement.

8.3.2 Processus d'évaluation de la sécurité et d'autorisation des TI

La conformité sera évaluée et validée par le Canada au moyen du processus d'évaluation de la sécurité et d'autorisation de la GRC ou d'un processus tiers déterminé par le Canada. Le processus d'évaluation et d'autorisation de sécurité de la GRC est fondé sur le guide ITSG-33 (https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie) et suit les pratiques exemplaires et les lignes directrices du Processus d'application de la sécurité dans les systèmes d'information (PASSI) du Centre canadien pour la cybersécurité (CCCS) (https://cyber.gc.ca/fr/orientation/annexe-2-activites-de-gestion-des-risques-lies-la-securite-des-systemes-dinformation)

Dans le cas où l'entrepreneur a été évalué et validé par l'entremise du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100) du Centre canadien pour la cybersécurité (CCC). (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux), l'entrepreneur doit démontrer qu'il a participé au processus en adhérant avec succès au programme, en y participant et en le terminant. Cela comprend le fait de fournir les documents suivants :

a) une copie de la lettre de confirmation qui indique qu'il a adhéré au programme;
b) une copie du dernier rapport d'évaluation rempli fourni par le CCC; et
c) une copie du dernier rapport sommaire fourni par le CCC.

8.3.3 Protection des données

L'entrepreneur doit :

a) mettre en œuvre le chiffrement de bout en bout pour toutes les données transférées au service de SGPN et en provenance de celui-ci, conformément à la section 8.3.8, Protection cryptographique;
b) mettre en œuvre le chiffrement des données inactives pour tous les services qui hébergent des données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés ou liés aux données organisationnelles, lorsque le chiffrement des données inactives demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie, conformément à la section 8.3.8, Protection cryptographique;
c) transmettre les données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés ou liés aux données organisationnelles, de manière sécuritaire, y compris la mise en œuvre du chiffrement des données en transit pour toutes les transmissions de données organisationnelles, conformément à la section 8.3.8, Protection cryptographique et à la section 8.3.13, Sécurité des réseaux et des communications;
d) Mettre en place des contrôles de sécurité qui restreignent l'accès administratif aux données organisationnelles à toutes les métadonnées ou à tous les journaux dérivés des données et des systèmes organisationnels ou connexes par l'entrepreneur et qui permettent d'exiger l'approbation du gouvernement du Canada avant que l'entrepreneur

puisse accéder aux données organisationnelles pour effectuer des activités de soutien, d'entretien ou d'exploitation;

e) prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continuels aux données organisationnelles, et que l'accès soit limité au personnel de l'entrepreneur selon le principe d'accès sélectif, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation du gouvernement du Canada;
f) empêcher tout employé de l'entrepreneur de détenir des justificatifs d'identité qui permettent à cet employé de supprimer, de modifier ou de copier des données organisationnelles à moins que cette personne n'ait été autorisée par la GRC au niveau approprié jugé nécessaire par cette dernière.

L'entrepreneur ne doit pas faire de copies des bases de données ou des parties de ces bases de données contenant des données organisationnelles à l'extérieur des capacités de résilience des services réguliers et dans les lieux ou zones régionaux approuvés au Canada.

L'entrepreneur ne doit pas déplacer ou transmettre les données organisationnelles au repos à l'extérieur des régions de service convenues, sauf lorsque l'approbation est obtenue de la GRC.

Sur demande du gouvernement du Canada, l'entrepreneur doit lui fournir un document qui détaille et décrit toutes les métadonnées créées à partir des données organisationnelles.

8.3.4 Supports amovibles/portables

Toutes les caméras corporelles et autres supports portables/amovibles doivent être validés et se conformer à la FIPS 140-2, niveau 1.

8.3.5 Emplacement des données

Conformément aux orientations contenues dans le document suivant : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/ligne-directrice-services-numerique.html#ToC4_4, l'entrepreneur doit stocker et protéger les données organisationnelles inactives, y compris les données dans des copies de sauvegarde ou conservées à des fins de redondance. Cela comprend la capacité d'isoler les données à l'intérieur des frontières géographiques du Canada avec un des fournisseurs de services infonuagiques (FSI) approuvé sur la liste suivante : https://cloud-broker.canada.ca/s/central-provider-page-v2?language=fr

L'entrepreneur ou le sous-traitant doit attester que :

a) le service et les opérations gérés du SGPN du SaaS, y compris la surveillance et le soutien, seront assurés par le gouvernement du Canada ou l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis;
b) l'entretien, la réparation et le soutien pour les caméras corporelles seront assurés par le gouvernement du Canada ou l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

L'entrepreneur doit mettre en œuvre la capacité pour le Canada d'isoler les données organisationnelles hébergées dans le FSI approuvé dans des centres de données géographiquement situés au Canada.

À la demande de la GRC et/ou du Canada, l'entrepreneur doit :

a) fournir à la GRC et/ou au Canada une liste à jour des emplacements physiques, y compris la ville, qui peuvent contenir les données organisationnelles pour chaque centre de données FSI qui sera utilisé pour fournir les services infonuagiques; et
b) indiquer les parties des services qui sont fournies depuis l'étranger, y compris tous les endroits où les données sont stockées et traitées et d'où l'entrepreneur gère le service;
c) fournir des preuves d'une certification tierce pour tous les emplacements physiques hébergeant des données organisationnelles à l'intérieur ou à l'extérieur du Canada.

Le fournisseur des Services proposés a l'obligation permanente d'aviser le gouvernement du Canada lorsque des mises à jour sont apportées à la liste des lieux physiques où peuvent se trouver les données organisationnelles.

8.3.6 Conservation des sauvegardes de données

L'entrepreneur doit s'assurer que :
a) Les sauvegardes de données sont conservées conformément à la politique de conservation de la GRC ou au moins pendant une période de cinq ans.
b) Processus de nettoyage.

8.3.7 Gestion des incidents de sécurité

Le processus d'intervention en cas d'incident de sécurité de l'entrepreneur pour le service doit englober le cycle de vie de la gestion des incidents de sécurité de la TI et les pratiques de soutien connexes pour les activités de préparation, de détection, d'analyse, de confinement et de reprise. Cela comprend notamment :
a) Un processus d'intervention en cas d'incident de sécurité publié et documenté pour examen par la GRC et/ou le Canada, qui est conforme à l'une des normes suivantes :
   i) ISO/IEC 27035:2011 Technologies de l'information -- Techniques de sécurité -- Gestion des incidents de sécurité de l'information;
   ii) NIST SP800-612, Computer Security Incident Handling Guide;
   iii) plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) (https://https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html);
   iv) autres pratiques exemplaires des normes de l'industrie, si la GRC détermine, à sa discrétion, qu'elles répondent à ses exigences relatives à la sécurité.
b) Des processus et des procédures documentés sur la façon dont l'entrepreneur détectera les incidents de sécurité de l'information, y donnera suite, y remédiera, les signalera et en fera part à la GRC et/ou au Canada, notamment :
   i) La portée des incidents de sécurité de l'information que l'entrepreneur signalera à la GRC et/ou au Canada; la quantité d'information communiquée sur la détection des incidents de sécurité de l'information et les interventions connexes; le délai prévu pour l'envoi des avis d'incident;
   ii) La procédure de transmission d'avis d'incident de sécurité de l'information;
   iii) Les coordonnées des personnes-ressources chargées du traitement des questions relatives aux incidents de sécurité de l'information;
   iv) Les recours qui s'appliquent si certains incidents de sécurité de l'information se produisent.

L'entrepreneur doit avoir mis en place des procédures pour répondre aux demandes relatives à des éléments de preuve numériques potentiels ou à d'autres renseignements provenant de l'environnement du service, ce qui comprend des procédures judiciaires et des mesures de protection pour assurer le maintien d'une chaîne de possession.

Si le Canada l'exige, l'entrepreneur doit :

a) travailler avec la GRC et le(s) centre(s) des opérations de sécurité du Canada (p. ex. le CCC, le COS de la GRC) au confinement et à l'élimination de l'incident de sécurité, et à la reprise des activités conformément au processus d'intervention en cas d'incident de sécurité;
b) tenir un registre des atteintes à la sécurité comprenant une description de l'atteinte, la durée, les conséquences de l'atteinte, le nom de la personne qui a signalé l'atteinte et celui de la personne à qui l'atteinte a été signalée, et la procédure pour récupérer les données ou le service;
c) assurer le suivi de la communication des données organisationnelles, ou permettre à la GRC et/ou au Canada d'en assurer le suivi, ce qui comprend le suivi des données qui ont été communiquées, et à qui et à quel moment elles ont été communiquées.

8.3.8 **Protection cryptographique**

L'entrepreneur doit :

a) configurer toute solution cryptographique qui est adoptée à l'égard des services et qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex. solutions liées au réseau privé virtuel, protocole TLS, modules logiciels, indicateurs de rendement clés et jetons d'authentification, le cas échéant), conformément avec les algorithmes cryptographiques, les tailles de clés de chiffrement et les périodes de validité des clés approuvés par le Centre de la sécurité des télécommunications (CST);
b) utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été validés par le Programme de validation des algorithmes cryptographiques;
c) (http://csrc.nist.gov/groups/STM/cavp/) et sont précisés dans le document ITSP.40.111 Algorithmes cryptographiques pour les renseignements non classifiés, protégés A et protégés B ou les versions subséquentes (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b);

L'entrepreneur doit s'assurer que :

a) qu'au moins une cryptographie validée de niveau 1 de la norme « Federal Information Processing Standards (FIPS) 140-2 » est utilisée lorsque le chiffrement est requis pour les caméras corporelles;

b) qu'au moins une cryptographie validée de niveau 1 de la norme FIPS 140.2 est utilisée lorsque le chiffrement est requis pour le SGPN.

Le cas échéant :

a) Tout chiffrement doit être mis en œuvre, configuré et exploité dans un module cryptographique validé par le Programme de validation des modules cryptographiques (https://cyber.gc.ca/fr/programme-de-validation-des-modules-cryptographiques-pvmc) en mode approuvé ou autorisé afin de fournir un degré élevé de certitude que le module cryptographique validé selon la norme FIPS 140-2 fournit les services de sécurité attendus de la manière prévue;

b) S'assurer que tous les modules FIPS 140-2 utilisés ont une certification active, à jour et valide. Les produits conformes/validés selon la norme FIPS 140-2 auront un numéro de certificat.

8.3.9 **Interfaces de programmation d'applications (API) externes**

L'entrepreneur doit :

a) fournir des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées pour prendre en charge des activités comme l'interopérabilité entre les composants et faciliter la migration des applications;

b) prendre les mesures appropriées pour protéger les API externes par des méthodes d'authentification sécurisées. Cela comprend s'assurer que toutes les requêtes d'API exposées à l'externe nécessitent une authentification réussie avant que celles-ci puissent être appelées et fournir au Canada la capacité de respecter les normes du gouvernement du Canada sur les API (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html).

8.3.10 **Gestion de l'identité et de l'accès**

L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge un accès sécurisé au service, y compris la capacité de configurer :

a) l'authentification multifactorielle conformément à l'ITSP.30.031 V3 du CST (ou versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de) à l'aide de justificatifs approuvés par le gouvernement du Canada;
b) un accès basé sur les rôles;
c) des contrôles de l'accès aux objets stockés; et
d) des politiques d'autorisation granulaire pour autoriser ou limiter l'accès.

L'entrepreneur doit avoir la capacité d'établir des paramètres par défaut à l'échelle de l'organisation pour gérer les politiques applicables à l'ensemble des locataires.

8.3.11 **Fédération**

L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge l'intégration fédérée de l'identité, y compris :

a) la prise en charge de normes ouvertes pour les protocoles d'authentification tels que le langage SAML (Security Assertion Markup Language) 2.0 ou OpenID Connect 1.0 (ou versions ultérieures), où les données d'identification et l'authentification de l'utilisateur final du service relèvent exclusivement du gouvernement du Canada; **et**
b) la capacité d'associer des identifiants uniques du Canada (p. ex. ID unique d'utilisateur final, adresse électronique d'utilisateur final) aux comptes d'utilisateurs correspondants du service infonuagique.

8.3.12 **Emplacement des employés de l'entrepreneur – Gestion des services à distance**

L'entrepreneur doit gérer et surveiller l'administration à distance du service de l'entrepreneur utilisé pour héberger les données organisationnelles, en prenant les mesures suivantes, sans s'y limiter :

a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs d'accès à distance, conformément à l'ITSP.30.031 V3 (ou versions ultérieures) du CST (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);
b) utiliser des terminaux à sécurité renforcée (p. ex. ordinateurs, dispositifs d'utilisateurs finaux, serveurs intermédiaires) configurés de façon à offrir une fonctionnalité minimale (p. ex. terminal spécialisé qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) afin d'assurer le soutien et l'administration des services et soutenir l'infrastructure de l'entrepreneur.

À la demande du Canada, l'entrepreneur doit fournir un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance de l'administration à distance des services.

8.3.13 **Sécurité des réseaux et des communications**

L'entrepreneur doit :

a) établir des connexions sécurisées au service, notamment en assurant la protection des données en transit entre le Canada et le Service au moyen de TLS 1.2 ou de versions ultérieures;
b) utiliser des protocoles, des algorithmes cryptographiques et des certificats à jour et pris en charge, comme il est décrit dans les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b) du CST;
c) utiliser des certificats correctement configurés dans les connexions TLS, conformément aux directives du CST (ITSP.40.111 du CST https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062)

8.3.14 **Accès et vérification**

L'entrepreneur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers de vérification des composantes de service du logiciel service (SaaS) sans s'y limiter :

a) Transmettre les événements et les journaux des locataires canadiens à un système de journaux de vérification centralisé géré par la GRC et/ou par le gouvernement du Canada en utilisant des interfaces de rapport, des protocoles et des formats de données normalisés (p. ex. Common Event Format [CEF], syslog ou autres formats courants de journaux) et des API qui permettent de récupérer à distance les données des journaux (p. ex. au moyen d'une interface de base de données utilisant SQL).
b) L'entrepreneur doit fournir des interfaces de programmation d'applications pour la composante de service SaaS qui permettent au Canada :
    i) d'inspecter et d'interroger les données inactives;
    ii) d'exporter les journaux d'événements de sécurité pour la ou les solutions; et
    iii) d'évaluer les événements stockés dans les journaux d'application. Cela comprend, sans s'y limiter, les événements tels que l'accès et le comportement

des utilisateurs, l'accès et le comportement des administrateurs, et les modifications de l'accès aux interfaces de protocole d'application de tiers, enregistrés dans les journaux d'application.

8.3.15 **Fuite d'information**

L'entrepreneur doit disposer d'un processus documenté décrivant son approche en cas d'incident de fuite de renseignements. Le processus doit être harmonisé avec :

a) les directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33;

b) une autre pratique exemplaire du secteur approuvée par écrit par la GRC ou le gouvernement du Canada.

Le processus d'intervention de l'entrepreneur en cas de fuite d'information doit comprendre, au minimum :

a) un processus pour informer le Canada de la possibilité d'une fuite d'information;
b) un processus d'identification des éléments de données précis qui sont en cause dans la contamination d'un système;
c) un processus pour isoler et éradiquer un système contaminé;
d) un processus d'identification des systèmes qui pourraient avoir été contaminés par la suite et toute autre mesure prise pour d'autres contaminations.

À la demande du Canada, l'entrepreneur doit fournir un document décrivant son processus d'intervention en cas de fuite de renseignements.

Dans le cas d'une fuite de renseignements repérée par la GRC, le gouvernement du Canada ou l'entrepreneur, ce dernier doit être en mesure de prendre les mesures énoncées à la 8.3.7 Gestion des incidents de sécurité.

8.3.16 **Test de sécurité et validation**

L'entrepreneur doit permettre que des tests d'évaluation des vulnérabilités internes soient effectués au besoin par le Canada ou par un tiers choisi par le Canada. Ces tests doivent être effectués au moins une fois par année et être conformes aux contrôles de gestion des vulnérabilités dans le Profil de contrôle de sécurité ministérielle de la GRC (PCSMG). L'entrepreneur et le Canada doivent s'entendre sur l'attribution de la responsabilité liée au soutien des tests d'évaluation des vulnérabilités.

8.3.17 **Vérifications des antécédents/Filtrage de sécurité du personnel**

L'entrepreneur et ses sous-traitants et sous-sous-traitants doivent collaborer avec le Canada ou toute tierce partie autorisée afin de déterminer les rôles auxquels des droits d'accès élevés sont attribués dans l'organisation de l'entrepreneur. Le personnel assumant ces rôles pourrait être soumis à des processus supplémentaires de filtrage de sécurité du personnel de la GRC. Si les employés de l'entrepreneur ayant des droits d'accès élevés ne répondent pas aux exigences liées aux niveaux d'autorisation de sécurité du personnel de la GRC indiqués, l'entrepreneur doit fournir à la GRC un plan en vue de doter les rôles en question par des employés répondant à ces exigences.

8.3.18 **Processus continu d'intégrité de la chaîne d'approvisionnement**

Traitement des préoccupations relatives à la sécurité

Si le gouvernement du Canada détermine, à sa discrétion, que la préoccupation relevée en matière de sécurité pose une menace à la fois grave et imminente pour la sécurité nationale, l'autorité contractante pourrait exiger que l'entrepreneur cesse immédiatement de déployer le ou les services ou produits désignés dans le contrat, selon un calendrier établi par le Canada. Cependant, avant de prendre une décision finale à cet égard, le Canada permettra à l'entrepreneur de répondre à la préoccupation relative à la sécurité dans les 48 heures suivant la réception de l'avis de l'autorité contractante. Par exemple, l'entrepreneur pourrait proposer des mesures d'atténuation que le Canada pourra considérer. Le Canada prendra ensuite une décision finale.

8.3.19 **Programme de sécurité industrielle – Exigences relatives à la sécurité pour les fournisseurs canadiens et étrangers**

L'entrepreneur doit respecter les dispositions de ce qui suit :

a) la liste de vérification des exigences relatives à la sécurité et le guide de sécurité (le cas échéant);
b) le Manuel de la sécurité industrielle (dernière édition);
c) le site Web de la Direction des services industriels des organisations (DSSIO) : Exigences de sécurité des contrats du gouvernement du Canada, à l'adresse https://www.tpsgc-pwgsc.gc.ca/esc-src/.

REMARQUE : Il peut y avoir plusieurs niveaux de filtrage de sécurité du personnel associés à ce dossier. L'entrepreneur doit consulter le guide de sécurité joint à la LVERS afin de clarifier ces niveaux de filtrage.

8.4 **Obligations en matière de confidentialité**

Les exigences en matière de protection des renseignements personnels seront peaufinées davantage à une étape ultérieure du processus d'approvisionnement.

8.4.1 **Certifications liées à l'assurance d'une tierce partie**

Une certification qui peut être examinée et prise en compte est :

a) La certification ISO/IEC 27018:2019 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

Acronymes, définitions et interprétation

APF	Expression qui signifie « **Authentification par plusieurs facteurs** », qui est une méthode d'authentification par laquelle un utilisateur d'ordinateur n'obtient l'accès qu'après avoir réussi à présenter deux ou plusieurs éléments de preuve à un mécanisme d'authentification.
CABR	« **Contrôle d'accès basé sur les rôles** » désigne le contrôle d'accès basé sur les rôles des utilisateurs (c.-à-d. un ensemble d'autorisations d'accès qu'un utilisateur reçoit en fonction d'une hypothèse explicite ou implicite sur un rôle donné). Les autorisations selon le rôle peuvent être héritées par une hiérarchie de rôles et reflètent généralement les autorisations nécessaires pour exécuter des fonctions définies au sein d'une organisation. Un rôle donné peut s'appliquer à une seule personne ou à plusieurs personnes. (nist.gov)
Caviardage	Le « **Caviardage** » signifie masquer ou supprimer des parties d'un texte avant sa publication ou distribution.
CCC	Le « **Centre canadien pour la cybersécurité** » est un organisme gouvernemental qui aide à renforcer la résilience et la sécurité du Canada en matière de cybersécurité par l'entremise de ses conseils, de son orientation, de son expertise et de ses partenariats. Le CCC offre un guichet unique de conseils et de services d'experts aux gouvernements, aux exploitants d'infrastructures essentielles et aux secteurs public et privé pour renforcer leur cybersécurité. (www.cyber.gc.ca/fr)
CST	**Centre de la sécurité des télécommunications.** Il s'agit de l'organisme national de cryptologie du gouvernement du Canada. Administré par le ministère de la Défense nationale, il est responsable des renseignements électromagnétiques étrangers et de la protection des réseaux électroniques d'information et de communication du gouvernement du Canada.
DACW	**Directives pour l'accessibilité aux contenus Web.** Elles ont été élaborées par l'intermédiaire du processus W3C en collaboration avec des particuliers et des organisations des quatre coins du monde, dans le but de présenter une norme commune unique dans le domaine de l'accessibilité des sites Web qui répond aux besoins des particuliers, des organisations et des gouvernements à l'échelle internationale.
Données organisationnelles	Les **données organisationnelles** désignent toutes les données créées ou traitées par la GRC, ses organismes partenaires ou le Canada dans le service d'informatique en nuage. Les données organisationnelles comprennent toutes les métadonnées et les journaux dérivés ou liés aux données organisationnelles.
DP	Expression qui signifie « **demande de propositions** », qui est un document d'invitation à soumissionner formulée par voie d'appel d'offres, par un organisme intéressé à acheter un produit, un service ou un actif précieux auprès de fournisseurs éventuels afin de soumettre des propositions commerciales.
DR	**Demande de renseignements**
ESA	Expression qui désigne l'**évaluation de sécurité et autorisation**, qui est le mécanisme par lequel le risque pour un système de TI est compris, atténué et géré de façon constante et mesurable tout au long de son cycle de vie.
FSI	**« Fournisseur de services infonuagiques »** désigne l'entité qui possède, exploite et entretient l'infrastructure (« nuage ») et fournit des ressources informatiques virtualisées aux consommateurs. Le FSI peut fournir une infrastructure informatique de base telle que le calcul et le stockage des données ou des solutions complètes sous forme de logiciels hébergés.

Fuite de renseignements	**Fuite de renseignements** désigne des incidents où une ressource d'information est déposée par inadvertance dans un dispositif ou dans un système qui n'est pas autorisé à traiter ces renseignements (LDSTI-33, IR-9).
GC	**Gouvernement du Canada.**
GRC	S'entend de la **Gendarmerie royale du Canada**, qui est le service national de police du Canada et qui assure l'application de la loi au niveau fédéral. La GRC assure également des services de police provinciaux dans huit provinces du Canada (Alberta, Colombie-Britannique, Manitoba, Nouveau-Brunswick, Terre-Neuve-et-Labrador, Nouvelle-Écosse, Île-du-Prince-Édouard et Saskatchewan, c.-à-d. toutes les provinces sauf l'Ontario et le Québec) et des services de police locaux sur une base contractuelle dans les trois territoires (Territoires du Nord-Ouest, Nunavut et Yukon) et dans plus de 150 municipalités, 60 communautés autochtones et trois aéroports internationaux.
IaaS	« **Infrastructure comme service** » signifie une méthode de prestation de service d'infonuagique par laquelle un fournisseur de services infonuagiques fournit au consommateur des ressources informatiques de base comme des serveurs, le traitement, le stockage et la mise en réseau qui lui permettent de déployer et de faire fonctionner des logiciels arbitraires, y compris des systèmes d'exploitation et des applications. Le consommateur ne gère pas ou ne contrôle pas l'infrastructure en nuage sous-jacente, mais maîtrise des systèmes d'exploitation, le stockage et des applications mises en place, et maîtrise peut-être partiellement certaines composantes de réseautage (p. ex. les pare-feu hôtes).
Incident de sécurité	« **Incident de sécurité** » désigne toute anomalie observable ou mesurable survenant à l'égard d'un bien, qui entraîne ou peut entraîner : (A) une violation des politiques de sécurité du Canada, une mesure de sécurité particulière, des politiques ou procédures de sûreté du fournisseur ou du sous-traitant fournisseur, ou toute exigence de ces obligations de sûreté ou des obligations en matière de protection des renseignements personnels ou (B) l'accès, la modification ou l'exfiltration non autorisés des titres de compétence du personnel autorisé, des titres de compétence des utilisateurs ou des biens d'information.
IPA	**Interface de programmation d'applications** désigne une interface qui permet aux développeurs d'interagir avec les programmes et les applications, y compris les systèmes de gestion de l'apprentissage.
IQ	**Invitation à se qualifier**
LVERS	**Liste de vérification des exigences relatives à la sécurité**
Métadonnées	« **Métadonnées** » signifie des données qui fournissent des renseignements sur d'autres données.
PaaS	La **plateforme en tant que service** est une méthode de prestation de service d'infonuagiques : un fournisseur de services infonuagiques (FSI) fournit une plateforme sur laquelle le consommateur peut créer, offrir et soutenir des applications et des services sur Internet. Les serveurs, le système d'exploitation et d'autres services comme les bases de données et les intergiciels sont gérés par le FSI.
PASSI :	**Processus d'application de la sécurité dans les systèmes d'information**
PCSMG	**Profil de contrôle de la sécurité ministérielle de la GRC**
PSC, TPSGC	Le **PSC, TPSGC** désigne le **Programme de sécurité des contrats**, Travaux publics et Services gouvernementaux Canada de SPAC.
SaaS	Le « **logiciel en tant que service** » est un modèle de distribution de logiciels dans lequel le client paie par abonnement l'accès à une application qui est hébergée par un fournisseur de services infonuagiques (FSI). Le service est offert sur Internet.

SCT	**Secrétariat du Conseil du Trésor du Canada.** Il fournit des conseils et des recommandations au comité de ministres du Conseil du Trésor sur la façon dont le gouvernement investit dans les programmes et les services, ainsi que sur la façon dont il en assure la réglementation et la gestion.
SE	**Surveillant de l'équité**
Services infonuagiques	Le terme « **services infonuagiques** » désigne un style de calcul dans lequel les capacités évolutives et élastiques d'utilisation de l'informatique sont fournies en tant que service utilisant les technologies Internet. (Gartner.com)
SGPN	**Système de gestion des preuves numériques**
Solution ou solution SaaS	« **Solution** », « **solution de SaaS** » désigne l'application logicielle livrée selon un modèle de distribution de logiciels-service dans lequel un fournisseur de services applicatifs ou un fournisseur de services infonuagique met à la disposition des clients des applications logicielles hébergées de manière centralisée sur Internet, permettant ainsi l'accès à la solution mise à jour et actualisée, aux services de soutien technique, à l'infrastructure de technologie de l'information sécurisée physiquement et électroniquement, le tout compris dans le service d'abonnement.
Sous-traitant	Le « **sous-traitant** » désigne la personne physique ou morale, l'autorité publique, l'organisme ou une autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données.
SPAC ou TPSGC ou **Services publics et Approvisionnement Canada** ou **Travaux publics et Services gouvernementaux Canada**	« **SPAC** » ou « **TPSGC** » ou « **Services publics et Approvisionnement Canada** » ou « **Travaux publics et Services gouvernementaux Canada** » fait référence à Services publics et Approvisionnements Canada, comme prévu dans la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*.
Registre des incidents de sécurité	Le « **registre des incidents de sécurité** » renvoie à tout incident, tout avis ou toute alerte qu'un dispositif, un système ou un logiciel peut techniquement produire en ce qui concerne son état, ses fonctions et ses activités. Les registres des incidents de sécurité ne se limitent pas aux dispositifs de sécurité; ils s'appliquent à tous les dispositifs, systèmes et logiciels ayant techniquement la capacité de produire des registres sur les incidents pouvant être utilisés dans les enquêtes sur la sécurité, les vérifications et les activités de surveillance. Voici quelques exemples de systèmes qui peuvent produire des journaux d'événements de sécurité : pare-feu, systèmes de prévention d'intrusion, routeurs, commutateurs, filtrage de contenu, registres du flux de trafic d'un réseau, réseaux, services d'authentification, services de répertoire, protocoles DHCP, systèmes DNS, plateformes matérielles, plateformes de virtualisation, serveurs, systèmes d'exploitation, serveurs Web, bases de données, applications, pare-feu à couche application (couche 7).
RQ	**Répondants qualifiés**
VOD	**Vérification d'organisation désignée**

ANNEXE B

CRITÈRES D'ÉVALUATION OBLIGATOIRES

1. Exigences obligatoires

1.1 Les Répondants doivent satisfaire à toutes les exigences obligatoires figurant dans la présente Annexe B conformément à la Partie 4 - Procédures d'évaluation et méthode de sélection de l'Invitation à se qualifier (ISQ).

2. Justification de la conformité – Critères d'évaluation obligatoires

2.1. Les Répondants doivent répondre aux exigences obligatoires correspondantes en expliquant, en démontrant et en justifiant leur expérience et leurs qualifications. Les réponses du Répondant aux exigences obligatoires seront évaluées conformément à la Partie 4 - Procédures d'évaluation et méthode de sélection de l'ISQ. Le Processus de conformité des soumissions par étapes s'appliquera à tous les critères obligatoires.

2.2. Les Répondants doivent soumettre un « Formulaire 2 – formulaire de vérification des projets cités en référence » dûment rempli pour chaque projet cité en référence en réponse au critère obligatoire correspondant.

2.3 Les répondants doivent seulement inclure le nombre de projets cités en référence demandés, tel qu'il est indiqué dans chaque critère obligatoire. Si le nombre de projets cités en référence fournis est supérieur au nombre requis, les soumissionnaires seront invités à identifier le ou les projets cités en référence à évaluer dans le délai spécifié par l'autorité contractante.

2.4 Pour satisfaire à l'un ou l'autre des critères d'évaluation technique O1, O2 et O3, en plus de sa propre expérience, le répondant peut soumettre l'expérience de l'une ou l'autre des entités suivantes (collectivement, « membre(s) de l'équipe ») :

a) une société mère ou une filiale du répondant;

b) un partenaire de coentreprise du répondant;

c) une filiale de la société mère du répondant;

d) une association d'entités.

Une association d'entités englobe les entités juridiques distinctes au sein d'un réseau officiellement organisé dont tous les membres fonctionnent en utilisant une image de marque commune. L'accès à la propriété intellectuelle et aux ressources de talent doit être partagé et la technologie, la méthodologie, les stratégies et les politiques doivent être intégrées à l'échelle du réseau.

2.4.1 Lorsqu'un répondant cite l'expérience d'un membre de l'équipe, le répondant doit démontrer que si cette expérience est accessible au répondant et que celui-ci peut compter sur l'expérience en question et s'en servir tout au long de la réalisation de tout contrat subséquent. Si l'expérience d'un membre de l'équipe est invoquée, le répondant est tenu de l'inclure dans sa réponse aux critères O1, O2 et O3 :

a) le nom légal du ou des membres de l'équipe qui ont effectué le travail ou fournir les services sur lesquels ils s'appuient pour démontrer leur expérience;

b) une description détaillée de la relation entre le ou les membres de l'équipe et le répondant;

c) une démonstration de la manière dont le soumissionnaire pourra s'appuyer sur l'expérience du ou des membres de l'équipe et l'utiliser dans l'exécution de tout contrat résultant.

2.4.2 Les répondants devraient inclure ce qui suit dans leur réponse :

a) un document justifiant la relation d'affaires avec les membres de l'équipe;

b) un accord entre le répondant et les membres de l'équipe établissant la manière dont ceux-ci engageront leur expérience dans l'exécution de tout contrat résultant.

Si le répondant ne soumet pas la documentation mentionnée aux points 2.4.2 a) et b) avec sa réponse, le Canada peut donner aux répondants la possibilité de soumettre la documentation. Il est obligatoire de fournir la documentation si elle est demandée, et selon les conditions demandées.

Critère	Critères obligatoires	Évaluation	Preuve requise
O1	**Projets cités en référence pour les caméras d'intervention** Le Répondant doit présenter au moins un (1) et jusqu'à quatre (4) projets cités en référence dans le cadre desquels, au minimum, le Répondant a fourni et distribué à des organismes d'application de la loi un total de 11 000 caméras d'intervention, y compris les services d'entretien, de soutien et de formation. • L'un des projets cités en référence doit avoir été d'une durée d'au moins une (1) année* au cours des cinq (5) années précédant la date de clôture de l'ISQ. • L'un (1) des projets cités en référence doit avoir porté sur la fourniture et la distribution d'au moins 5 000 caméras d'intervention. • Tous les projets cités en référence doivent avoir compris la fourniture et la distribution de caméras d'intervention. • Tous les projets cités en référence doivent avoir compris la prestation	Satisfait/ non satisfait	Le Répondant doit présenter les renseignements suivants pour chaque projet cité en référence : • nom de l'organisme d'application de la loi; • description des biens et des services fournis; • dates et période de fourniture des biens et des services; • pour que le Canada puisse effectuer la vérification des références, le Répondant doit présenter les renseignements suivants pour chaque projet cité en référence : • nom de la personne-ressource; • titre; • adresse de courriel; • numéro de téléphone.

	de services de soutien et d'entretien des caméras d'intervention, y compris le soutien technique offert en tout temps par téléphone, par courriel ou en ligne en cas de mauvais fonctionnement, d'erreur ou de défectuosité de l'équipement. • Tous les projets cités en référence doivent avoir compris la prestation de services de formation en matière de caméras d'intervention, notamment : a) des séances de formation des formateurs; b) la création d'outils de formation, comme des cours en ligne ou des documents de référence. *Une (1) année correspond à une période de douze (12) mois consécutifs se terminant au plus tard à la date de clôture de l'ISQ.		Si la personne-ressource n'est pas disponible pour la vérification des références lors de l'évaluation, le Canada suivra la procédure prévue à l'article 4.3 – vérification des références de l'ISQ.
O2	**Projets cités en référence pour le système de gestion des preuves numériques (SGPN)** Le Répondant doit présenter au moins un (1) et jusqu'à quatre (4) projets cités en référence dans le cadre desquels, au minimum, le Répondant a fourni des services relatifs à un SGPN à des organismes d'application de la loi pour un total de 11 000 utilisateurs finaux. • L'un (1) des projets cités en référence doit avoir été d'une durée d'au moins une (1) année* au cours des cinq (5) années précédant la date de clôture de l'ISQ • Le SGPN doit avoir été déployé selon le modèle SaaS dans le cadre de tous les projets cités en référence. • Dans le cadre de tous les projets cités en référence, le SGPN déployé doit avoir été doté des capacités suivantes : a) stockage des enregistrements audio et vidéo	Satisfait/ non satisfait	Pour chaque projet cité en référence, le Répondant doit présenter les renseignements suivants : • nom de l'organisme d'application de la loi; • description des capacités et des services fournis; • dates et période de prestation des services. Pour que le Canada puisse effectuer la vérification des références, le Répondant doit présenter les renseignements suivants pour chaque projet cité en référence : • nom de la personne-ressource; • titre; • adresse de courriel; • numéro de téléphone. Si la personne-ressource n'est pas disponible pour la vérification

	provenant des caméras d'intervention; b) recherche et extraction de preuves numériques; et c) caviardage. • Tous les projets cités en référence doivent avoir compris des services de mise en œuvre démontrant en quoi le Répondant a aidé le client à réaliser les tâches suivantes : a) planification; b) configuration; c) mise à l'essai; et d) intégration progressive. • Tous les projets cités en référence doivent avoir compris la prestation de services de formation relatifs au SGPN, notamment : a) des séances de formation des formateurs et b) la création d'outils de formation, comme des cours en ligne ou des documents de référence. • Tous les projets cités en référence doivent avoir compris des services de soutien et d'entretien du SGPN, notamment : a) le soutien technique offert en tout temps par téléphone, par courriel ou en ligne en cas de problème de rendement, d'erreur ou de défectuosité de l'application; b) les mesures correctives (p. ex. correction de bogues) et/ou les correctifs pour l'application; et c) les services continus de mise à niveau de l'application. *Une (1) année correspond à une période de douze (12) mois consécutifs se terminant au plus tard à la date de clôture de l'ISQ.		des références lors de l'évaluation, le Canada suivra la procédure prévue à l'article 4.3 – vérification des références de l'ISQ. Remarque : Le Répondant peut citer en référence les mêmes projets qu'au critère O1, mais les projets doivent satisfaire aux exigences décrites au critère O2.
O3	**Projets cités en référence pour le service intégré de caméras d'intervention et de SGPN** Le Répondant doit présenter au moins un (1) et jusqu'à trois (3) projets cités en référence dans le cadre desquels, au minimum, le Répondant a fourni des	Satisfait/ non satisfait	Pour chaque projet cité en référence, le Répondant doit présenter les renseignements suivants : • nom de l'organisme d'application de la loi;

	services intégrés de caméras d'intervention et de SGPN à des organismes d'application de la loi pour un total de 3 000 utilisateurs finaux. • L'un (1) des projets cités en référence doit avoir été d'une durée d'au moins une (1) année* au cours des cinq (5) années précédant la date de clôture de l'ISQ. Tous les projets cités en référence doivent avoir compris les services intégrés de caméra d'intervention et de SGPN suivants : • téléversement automatisé des données audio et vidéo de la caméra d'intervention vers le SGPN depuis la station d'accueil. *Une (1) année correspond à une période de douze (12) mois consécutifs se terminant au plus tard à la date de clôture de l'ISQ.		• description des biens, des capacités et des services fournis; • dates et période de prestation des services. Pour que le Canada puisse effectuer la vérification des références, le Répondant doit présenter les renseignements suivants pour chaque projet cité en référence : • nom de la personne-ressource; • titre; • adresse de courriel; • numéro de téléphone. Si la personne-ressource n'est pas disponible pour la vérification des références lors de l'évaluation, le Canada suivra la procédure prévue à l'article 4.3 – vérification des références de l'ISQ. Remarque : Le Répondant peut citer en référence les mêmes projets qu'aux critères O1 et O2, mais les projets doivent satisfaire aux exigences décrites au critère O3.
O4	Le droit de propriété intellectuelle du volet SGPN nécessaire à la prestation du service proposé (à l'exception des additifs et des extensions) au Canada doit appartenir au Répondant (ou dans le cas d'une coentreprise, à l'une des personnes ou des entités). Ainsi, le Répondant peut apporter des améliorations au produit commercial principal et en assurer le soutien en vue de répondre aux besoins du gouvernement du Canada (GC).	Satisfait/ non satisfait	Le Répondant doit donner une courte description de moins d'une page indiquant en quoi il satisfait aux critères. De plus, le Répondant doit présenter dans le cadre de sa réponse une attestation certifiant qu'il est l'éditeur du logiciel-service proposé et qu'il possède tous les droits nécessaires pour accorder des licences d'exploitation du service au Canada (Formulaire 3 – Formulaire d'attestation de

			l'éditeur de logiciels-services SaaS).
O5	Le service de SGPN proposé par le Répondant doit permettre aux utilisateurs finaux de travailler dans les deux langues officielles du Canada (anglais et français) pendant la durée du contrat. Si la solution proposée ne permet pas aux utilisateurs de travailler dans les deux langues officielles du Canada (anglais et français) à la date de clôture de l'ISQ, le Répondant doit fournir une feuille de route démontrant que les services de SGPN seront offerts dans les deux langues officielles du Canada (anglais et français) avant la mise en œuvre de la solution.	Satisfait/ non satisfait	Si le service de SGPN proposé permet aux utilisateurs finaux de travailler dans les deux langues officielles du Canada (anglais et français) à la date de clôture de l'ISQ, le Répondant doit présenter une courte description de moins d'une page indiquant en quoi il satisfait aux critères, ainsi que les éléments suivants, dans les deux langues officielles du Canada (anglais et français) : 1) une capture d'écran d'une page de recherche générale; 2) un guide de l'utilisateur. Si la solution proposée ne permet pas aux utilisateurs finaux de travailler dans les deux langues officielles du Canada (anglais et français) à la date de clôture de l'ISQ, le Répondant doit présenter une feuille de route de haut niveau, sur laquelle figure le calendrier de mise en œuvre des principales caractéristiques et capacités du produit dans les deux langues officielles du Canada (anglais et français), y compris le soutien technique, l'interface utilisateur du SGPN, l'interface utilisateur des caméras d'intervention, les ressources de formation et les documents sur le produit.
O6	Le Répondant doit démontrer que le volet SGPN du service proposé est offert selon un modèle SaaS, comme le définit le document special publication 800-145 du National Institute of Standards and Technology.	Satisfait/ non satisfait	Pour démontrer qu'il satisfait à cette exigence, le Répondant doit donner une courte description de moins d'une page indiquant en quoi le service proposé satisfait aux critères.

O7	Le Répondant doit démontrer qu'il a lu et qu'il comprend les exigences en matière d'accessibilité énoncées ci-dessous : • les normes des Règles pour l'accessibilité des contenus Web (WCAG) 2.1, telles qu'elles sont décrites à l'adresse suivante : https://www.w3.org/TR/WCAG21/ ; • la Norme sur l'accessibilité des sites Web du gouvernement du Canada, telle qu'elle est décrite à l'adresse suivante : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601; • la Stratégie sur l'accessibilité au sein de la fonction publique du Canada, telle qu'elle est décrite à l'adresse suivante : https://www.canada.ca/fr/gouvernement/fonctionpublique/mieux-etre-inclusion-diversite-fonction-publique/diversite-equite-matiere-emploi/accessibilite-fonction-publique/strategie-accessibilite-fonction-publique-tdm.html. • la *Loi canadienne sur l'accessibilité* (https://www.parl.ca/DocumentViewer/fr/42-1/projet-loi/C-81/sanction-royal) – La *Loi canadienne sur l'accessibilité* a été promulguée dans le but de favoriser la participation pleine et égale dans la société de toutes les personnes, en particulier les personnes handicapées. La Loi vise à parvenir à cette fin par la transformation du Canada, dans le champ de compétence législative du Parlement, en un pays exempt d'obstacles, particulièrement par la reconnaissance, l'élimination et la prévention d'obstacles. • la Ligne directrice sur l'utilisabilité de la technologie de l'information (TI) par tous (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32620) – Cette ligne directrice vient appuyer	Satisfait/ non satisfait	Pour démontrer qu'il satisfait à cette exigence, le Répondant doit soumettre le Formulaire 1 – Formulaire de déclaration et de présentation de la réponse du Répondant pour confirmer qu'il a lu et qu'il a compris les exigences en matière d'accessibilité énoncées dans les normes des Règles pour l'accessibilité des contenus Web (WCAG) 2.1, la Norme sur l'accessibilité des sites Web du gouvernement du Canada et la Stratégie sur l'accessibilité au sein de la fonction publique du Canada.

	l'orientation du gouvernement du Canada visant à ce que les ministères, les organismes et les organisations tiennent compte de l'accessibilité dans l'acquisition ou l'élaboration de solutions et d'équipement de la technologie de l'information (TI), afin de rendre la TI accessible à tous.		
O8	Le Répondant doit démontrer que le volet SGPN du service proposé sera déployé dans l'environnement de l'un des fournisseurs de services infonuagiques approuvés par le GC pour les données de niveau Protégé B (https://cloud-broker.canada.ca/s/central-provider-page-v2?language=fr) d'ici à la date de clôture de l'ISQ. Le service du Répondant qualifié devra satisfaire aux exigences du Canada en matière de sécurité énoncées dans la Liste de vérification des exigences relatives à la sécurité (LVERS) qui figurera dans le document de demande de soumissions.	Satisfait/ non satisfait	Le Répondant doit soumettre une attestation certifiant qu'il héberge son service dans l'environnement d'un fournisseur de services infonuagiques approuvé par le GC pour les données de niveau Protégé B (Formulaire 4 – Formulaire d'autorisation du fournisseur de services infonuagigues du Gouvernement du Canada).

ANNEXE C:

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M7594-212120
Security Classification / Classification de sécurité Protected A

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: RCMP	2. Branch or Directorate / Direction générale ou Direction: CFO + IM/IT - NHQ / CIO / ED / PPM + C&IP
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The work to be performed includes delivering a Body Worn Camera (Equipment) and Digital Evidence Management System (SaaS) Program as a Managed Service. For the BWC, we expect the work to include full lifecycle management of the cameras from acquisition to disposal. For the DEMS, we expect a turnkey SaaS solution and professional services to link the DEMS with the RCMP's operational records management systems.

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

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

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

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

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

No release restrictions Aucune restriction relative à la diffusion ☐	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays : 5 Eyes Countries-New Zealand,Australia,UnitedKingdom,United States, Canada	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M7594-212120
Security Classification / Classification de sécurité Protected A

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

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

Special comments:
Commentaires spéciaux : See Security Guide which includes Classification Guidance

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

10. b) May unscreened personnel be used for portions of the work? — ☐ No / Non ☑ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — ☐ No / Non ☑ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M7594-212120
Security Classification / Classification de sécurité
Protected A

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens		✓														
Production		✓														
IT Media / Support TI		✓														
IT Link / Lien électronique		✓														

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Guide sur la sécurité de la LVERS

Caméras d'intervention et gestion des preuves numériques
LVERS nº : 202102120/M7594212120

Préambule

Tous les entrepreneurs visés par le présent contrat doivent respecter le contexte en matière de sécurité de la GRC en se conformant aux directives décrites dans le présent document. Une obligation plus détaillée en matière de sécurité sera fournie à l'étape Demande de proposition.

Exigences générales de sécurité

1. Tous les renseignements protégés (documentation papier) et tout autre bien de nature délicate dont la GRC a la responsabilité doivent être communiqués à l'entrepreneur conformément aux processus déjà approuvés.

2. Les renseignements divulgués par la GRC doivent être administrés, conservés et éliminés conformément aux dispositions du contrat. À tout le moins, l'entrepreneur doit respecter les dispositions de la Politique sur la sécurité du gouvernement.

3. L'entrepreneur doit rapidement aviser l'autorité responsable des contrats de la GRC de tout incident de sécurité lié aux renseignements fournis par la GRC (soit la perte accidentelle ou délibérée de renseignements de nature délicate).

4. Il est interdit de prendre des photos. Si des photos sont requises, veuillez communiquer avec l'autorité contractante et la Section de la sécurité ministérielle.

5. L'entrepreneur n'est pas autorisé à divulguer des renseignements de nature délicate reçus de la GRC à un sous-traitant n'ayant pas la cote de sécurité de la GRC requise pour accéder aux renseignements en question.

6. La Section de la sécurité ministérielle de la GRC se réserve le droit de mener des inspections dans les installations de l'entrepreneur et de fournir des conseils sur les mesures de protection obligatoires (mesures précisées dans le présent document et possiblement d'autres mesures propres au site). Ces inspections peuvent être réalisées avant que des renseignements de nature délicate ne soient divulgués ou selon les besoins (p. ex. si l'entrepreneur déménage ses bureaux). Ces inspections visent à assurer la qualité des mesures de protection mises en place.

7. Pour assurer le contrôle souverain du Canada sur ses propres données, toutes les données protégées ou de nature délicate sous contrôle gouvernemental seront conservées sur des serveurs situés au Canada. Les données en transit et au repos seront chiffrées de manière appropriée.

8. Les exigences en matière d'autorisation de sécurité pour le personnel des entrepreneurs et des fournisseurs seront établies en fonction des rôles anticipés et de l'accès aux données et aux systèmes du GC, conformément au Guide sur la classification de sécurité, à l'annexe A.

Sécurité matérielle

1. **Conservation** : Les renseignements et les biens protégés doivent être conservés dans un classeur approuvé par les responsables de la sécurité de la GRC. Le classeur doit être situé (au minimum) à l'intérieur d'une « zone de travail ». Par conséquent, les installations de l'entrepreneur doivent comprendre une zone ou une pièce Répondant aux critères suivants :

Zone des opérations	
Définition	Aire dont l'accès est limité au personnel qui y travaille et aux visiteurs accompagnés comme il se doit. Remarque : Le personnel travaillant dans la zone de travail doit : • posséder une cote de fiabilité approfondie; ou • être accompagné par une personne possédant une cote de fiabilité de la GRC valide.
Périmètre	Doit être délimité par un périmètre visible ou par un périmètre de sécurité, selon les besoins du projet. Par exemple, les commandes doivent se trouver dans une pièce ou un bureau fermé à clé.
Surveillance	Surveillance périodique par des employés autorisés. Par exemple, les utilisateurs de la zone de travail peuvent constater s'il y a eu infraction à la sécurité.

Remarque : Consulter l'annexe A pour obtenir de plus amples renseignements sur le concept de zone de sécurité.

2. **Discussions** : Lorsque l'on prévoit qu'il y aura des conversations de nature délicate, la zone de travail doit être séparée des aires publiques ou être dotée de propriétés acoustiques garantissant que les conversations pourront être tenues en privé (les utilisateurs doivent pouvoir s'attendre raisonnablement à ne pas être entendus). Il s'agit par exemple d'une salle ou d'un bureau privé ou bien d'une salle de conférence.

3. **Production** : La production (création ou modification) de renseignements ou de biens protégés doit se faire dans une aire Répondant aux critères exigés pour une zone de travail.

4. **Destruction** : Toutes les ébauches et les impressions erronées (copies endommagées ou excédentaires) doivent être détruites par l'entrepreneur. Les renseignements protégés doivent être détruits conformément aux dispositions du Manuel de la sécurité de la GRC. L'équipement ou le système (déchiqueteur) employé pour détruire les documents de nature délicate doit être coté conformément au degré de destruction requis. Il faut employer du matériel de destruction approuvé par la GRC.

   Le niveau de destruction approuvé pour les renseignements « Protégé B » est le suivant :
   - La taille des résidus ne doit pas dépasser 1 mm sur 14,3 mm (découpage en particules).

   Remarque :
   - Si l'entrepreneur n'est pas en mesure de répondre aux exigences de la GRC en matière de destruction, tous les renseignements et les biens de nature délicate doivent être retournés à la GRC pour leur destruction adéquate.
   - Toute ébauche ou impression manquée de renseignements de nature délicate en attente d'élimination doit être protégée de la façon convenue jusqu'à sa destruction.

5. **Transport ou transmission :** Pour l'échange physique de renseignements de nature délicate, il faut s'assurer que les données sont chiffrées avant leur transport et leur transmission. Le service de livraison utilisé, le cas échéant, doit fournir une preuve d'expédition, un suivi pendant l'expédition et une attestation de 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 :

- En ce qui a trait au transport de renseignements « Protégé B » (à destination ou en provenance d'un lieu neutre de réunion ou d'entrevue), il est possible d'utiliser une valise ou un autre contenant de solidité égale ou supérieure au lieu d'une enveloppe. Une enveloppe ou un emballage double doit être utilisé pour protéger les articles fragiles ou pour garder intacts des colis encombrants, lourds ou aux formes irrégulières;
- Pour la transmission de renseignements « Protégé B » (Postes Canada ou courrier recommandé), l'adresse doit rester vague. Ajouter au besoin « À ouvrir uniquement par le destinataire » si le principe du besoin de savoir ou d'accéder le justifie.

Mesures de contrôle générales en sécurité des TI
Contrôle approprié des renseignements protégés

Transport et transmission

1. S'il est nécessaire de transporter des renseignements protégés de la GRC, un dispositif de stockage portatif conforme à la norme FIPS 140-2 et fourni par la GRC doit être utilisé, avec accès restreint au client (GRC) et au personnel de l'entrepreneur ayant reçu une autorisation de sécurité de la GRC. Le dispositif de stockage portatif respectant la norme FIPS 140-2 doit être remis en personne ou livré par un service de messagerie approuvé jusqu'aux bureaux de l'entrepreneur.
2. Le mot de passe pour le dispositif de stockage portatif doit être fourni verbalement, soit en personne ou par téléphone, et uniquement aux membres du personnel de l'entrepreneur ayant obtenu la cote de sécurité de la GRC.
3. Une personne ne peut pas envoyer ou recevoir de renseignements de nature délicate de la GRC d'une adresse courriel externe.
4. Si le traitement électronique de l'information protégée fournie par la GRC est nécessaire, l'entrepreneur doit s'assurer que :
   - les renseignements sont chiffrés lorsqu'ils ne sont pas utilisés;
   - les renseignements sont chiffrés pendant le transfert;
   - les mécanismes de contrôle de l'accès ont été mis en œuvre.

   Remarque : Un algorithme Répondant à une norme de chiffrement avancé (AES) utilisant des clés de 256 bits est approuvé pour le chiffrement des renseignements protégés.

Téléphonie

1. Toutes les communications vocales par téléphone cellulaire ou appareil mobile doivent s'en tenir à des renseignements de nature non délicate, sauf si le téléphone est spécialement conçu pour transmettre des renseignements de nature délicate et accrédité à cette fin.

Impression, numérisation et photocopies

2. Si des renseignements électroniques protégés de la GRC doivent être imprimés ou numérisés, l'entrepreneur doit posséder des ordinateurs, des imprimantes ou des numériseurs supplémentaires prévus à cette fin. L'équipement ne doit pas être relié au réseau local ou à Internet. Les lecteurs de disque des ordinateurs doivent être chiffrés de la manière approuvée par la GRC.

Conservation

3. La sauvegarde de renseignements protégés de la GRC, au besoin, est soumise aux mêmes lignes directrices de sécurité (chiffrement et contrôle de l'accès) que les renseignements originaux.
4. Les dossiers électroniques doivent être détruits conformément au protocole ITSG-06 : *Effacement et déclassification des supports d'information électroniques* (consulter l'adresse https://www.cse-cst.gc.ca/en/node/270/html/10572 pour obtenir de plus amples renseignements).
5. Tous les dispositifs de stockage fournis par la GRC et utilisés pendant la durée du contrat doivent être remis à la GRC immédiatement lorsque le contrat prendra fin.

Mesures de contrôle de sécurité élargies pour les caméras d'intervention et la gestion des éléments de preuve numériques

Mesures de contrôle de sécurité élargies pour les caméras d'intervention et la gestion des éléments de preuve numériques

La présente section donne les grandes lignes des mesures de contrôle de sécurité principales auxquelles devront se conformer les fournisseurs participant à l'appel d'offres relatives au contrat sur les caméras d'intervention et/ou la gestion des éléments de preuve numériques. Tous les fournisseurs doivent fournir des preuves démontrant leur capacité à répondre aux mesures de contrôle de sécurité décrites ci-dessous. En vertu des documents à l'appui sur la sécurité, les preuves peuvent comprendre :

1. des documents relatifs aux politiques, aux procédures ou aux normes;
2. des rapports de vérification de tiers produits par l'un des organismes de certification des normes de l'industrie acceptables;
3. des documents d'un sous-traitant ou d'un sous-sous-traitant, y compris une entreprise de très grande échelle.

Des renseignements sur les mesures de contrôle de sécurité individuelles sont disponibles ici : https://www.cyber.gc.ca/fr/orientation/annexe-3a-catalogue-des-controles-de-securite-itsg-33.

Remarque sur les mesures de contrôle de sécurité héritées

Le National Institute of Standards and Technology (NIST) définit les mesures de contrôle de sécurité communes comme étant « [TRADUCTION] les mesures de contrôle de sécurité dont la mise en œuvre entraîne une capacité en matière de sécurité qui peut être héritée par un ou plusieurs systèmes d'information organisationnels ». Les mesures de contrôle de sécurité sont réputées héritables par des systèmes d'information ou par des composants de système d'information si les systèmes ou composants reçoivent une protection par les mesures de contrôle ayant été mises en œuvre, mais que ces mesures de contrôle sont conçues, mises en œuvre, évaluées, autorisées et surveillées par des entités autres que les entités responsables des systèmes ou des composants, y compris des entités internes ou externes aux organismes où résident les systèmes ou les composants. Si des fournisseurs héritent de mesures de contrôle de sécurité de la part de sous-traitants ou de sous-sous-traitants, ils doivent l'indiquer et en fournir la preuve.

Voici un sommaire des mesures de contrôle de sécurité attendues qui seront décrites en de plus amples détails à l'étape de l'appel de propositions.

ID	Objectif de sécurité	Contrôles de sécurité
1.0	**Gestion de l'identité et de l'accès (GIA)** ***Objectif :*** *Mettre en œuvre des mécanismes de gestion de l'identité et de l'accès pour la solution.*	AC-1, AC-2, AC-2(1), AC-2 (2) AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9) AC-2(10), AC-2(11), AC-3, AC-4, AC-4(21), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(3) AC-6(5), AC-6(7), AC-6(8), AC-6(9), AC-6(10), AC-7, AC-8, AC-10, AC-11, AC-11(1), AC-12, AC-12(1), AC-14, AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-17(9), AC-17(100), AC-18, AC-18(1), AC-18(4), AC-18(5), AC-19, AC-19(4), AC-19(5), AC-20, AC-20(1), AC-20(2), AC-2, AC-22, AC-23, AC-24. IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(5), IA-2(6), IA-2(8), IA-2(11), IA-3, IA-4, IA-4(2), IA-4(3), IA-4(4), IA-5, IA-5(1), IA-5(2), IA-5(3), IA-5(4), IA-5(6), IA-5(7), IA-5(8), IA-5(11), IA-6, IA-7, IA-8
2.0	**Vérification** ***Objectif :*** *Mettre en œuvre un mécanisme de vérification de la solution.*	AU-1, AU-2, AU-2(3), AU-3, AU-3(1), AU-3(2), AU-5, AU-5(2), AU-6, AU-6(1), AU-6(2), AU-6(3), AU-6(10), AU-7, AU-7(1), AU-8, AU-8(1), AU-9, AU-9(2), AU-9(3), AU-9(4), AU-10, AU-11, AU-12, AU-14, AU-14(1)
3.0	**Protection des données** ***Objectif :*** *Mettre en œuvre des mécanismes pour protéger les données en transit et les données inactives.*	SC-8, SC-8(1), SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-15, SC-17, SC-28, SC-28(1)
4.0	**Réseautique** ***Objectif :*** *Mettre en œuvre des mécanismes pour établir des périmètres de réseau interne et externe et pour surveiller le trafic sur le réseau.*	AC-4, SC-7, SC-7(3), SC-7(4). SC-7(5), SC-7(7), SC-7(8), SC-7(10), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-7(19), SC-7(21) SC-8, SC-10
5.0	**Développement sécurisé** ***Objectif :*** *Restreindre les vulnérabilités de la solution et assurer l'intégrité des données.*	AC-12 CA-8 RA-5 SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(3), SA-4(7), SA-4(8), SA-4(9), SA-5, SA-8, SA-9, SA-9(1), SA-9(2), SA-9(4), SA-9(5), SA-10, SA-10(1), SA-11, SA-11(1), SA-11(2), SA-11(8), SA-12, SA-12(1), SA-121(2), SA-12(5), SA-12(7), SA-12(8), SA-12(9), SA-12(11), SA-15 SC-1, SC-2, SC-2(1), SC-4, SC-5, SC-6, SC-18, SC-18(3), SC-18(4), SC-19, SC-20, SC-21, SC-22, SC-23, SC-23(1), SC-39 SI-10, SI-11, SI-12, SI-15, SI-16

ID	Objectif de sécurité	Contrôles de sécurité
6.0	**Continuité des services** ***Objectif :*** *Mettre en œuvre les mécanismes de sécurité nécessaires pour permettre la continuité des services.*	CP-1, CP-2, CP-2(1), CP-2(3), CP-2(4), CP-2(5), CP-2(6), CP-2(8), CP-3, CP-4, CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(1), CP-8(2), CP-8(3), CP-8(5), CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-9(7), CP-10, CP-10(2), CP-10(4) MA-1, MA-2, MA-2(2), MA-3, MA-3(1), MA-3(2), MA-3(3), MA-4, MA-4(1), MA-4(2), MA-4(3), MA-4(6), MA-4(7), MA-5, MA-5(1), MA-6
7.0	**Gestion de la configuration** ***Objectif :*** *Mettre en œuvre les éléments liés à la sécurité de la gestion de la configuration.*	CM-1, CM-2, CM-2(1), CM-2(2), CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(4), CM-3(6), CM-4, CM-5, CM-5(1), CM-5(5), CM-5(6), CM-6, CM-6(1), CM-6(2), CM-7, CM-7, CM-7(1), CM-7(2), CM-7(5), CM-8, CM-8(1), CM-8(2), CM-8(3), CM-8(5), CM-9, CM-10, CM-10(1), CM-11 SA-22 SC-43 MP-1, MP-2, MP-3, MP-4, MP-5, MP-5(4). MP-6, MP-6(1), MP-6(2), MP-6(3), MP-7, MP-7(1), MP-8, MP-8(1)
8.0	**Opérations de sécurité** ***Objectif :*** *Mettre en œuvre des mécanismes des opérations de sécurité pour le service.*	IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-4(3), IR-4(6), IR-5, IR-5(1), IR-6, IR-6(1), IR-7, IR-7(1), IR-7(2), IR-8, IR-9, IR-9(1), IR-9(2), IR-9(3), IR-9(4) SI-1, SI-2, SI-2(1), SI-2(2), SI-2(3), SI-3(1), SI-3(2), SI-3(7), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(4), SI-4(5), SI-4(7), SI-4(11), SI-4(14), SI-4(16), SI-4(20), SI-4(22), SI-4(23) SI-5, SI-5(1), SI-5, SI-6, SI-7, SI-7(1), SI-7(5), SI-7(7), SI-8, SI-8(1), SI-8(2) PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-8
9.0	**Objectif de l'évaluation de sécurité :** *Autoriser l'utilisation du service aux fins de production.*	CA-1, CA-2, CA-2(1), CA-2(2), CA-2(3), CA-3, CA-3(2), CA-3(3), CA-3(5), CA-5, CA-6, CA-7, CA-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(5), CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-9(7), CP-10, CP-10(2), CP-10(4), CA-8, CA-8(1), CA-9 RA-1, RA-2, RA-3, RA-5, RA-5(1), RA-5(2), RA-5(3), RA-5(5), RA-5(6), RA-5(8)
10.0	**Objectif en matière de sécurité matérielle :** *Mettre en œuvre le contrôle de sécurité des mécanismes physiques et environnementaux du service*	PE-1, PE-2, PE-2(3), PE-3, PE-3(1), PE-3(2), PE-4, PE-5, PE-6, PE-6(1), PE-6(4), PE-8, PE-8(1), PE-9, PE-10, PE-11, PE-11(1), PE-12, PE-13, PE-13(2), PE-13(2), PE-13(3), PE-14, PE-14(2), PE-15, PE-15(1), PE-16, PE-17
11.0	**Objectif en matière de sécurité du personnel :** *Mettre en œuvre le contrôle de la sécurité du personnel pour le service*	PS-1, PS-2, PS-3, PS-3(3), PS-4, PS-4(2), PS-5, PS-6, PS-7, PS-8

Sécurité du personnel

1. Tout le personnel de l'entrepreneur et des sous-traitants doit obtenir de la GRC et maintenir une autorisation ou une cote de sécurité du personnel correspondant au niveau de classification du travail à réaliser tout au long du cycle de vie du contrat (conformément aux dispositions de la LVERS).

2. Si des employés n'ayant pas subi de filtrage de sécurité sont affectés à cette exigence, les rôles doivent être indiqués, puis approuvés par la GRC. Cela aura lieu après la sélection du fournisseur retenu.

3. L'entrepreneur sera tenu d'informer la GRC de toute modification relative au personnel en ce qui touche les exigences propres à la sécurité (par exemple, lorsqu'un employé détenant une attestation de sécurité quitte l'entreprise ou ne participe plus à l'exécution du contrat de la GRC, lorsqu'un nouvel employé doit obtenir une attestation de sécurité, ou encore lorsqu'un employé doit faire renouveler son attestation de sécurité).

4. Puisque le fournisseur et ses employés auront accès à des renseignements protégés ou classifiés, une autorisation de sécurité de la GRC au niveau approprié est requise.
   Le personnel de l'entrepreneur doit faire l'objet d'une vérification par la GRC avant de se voir accorder l'accès à des renseignements protégés ou classifiés, aux systèmes, aux biens et/ou aux installations. La GRC se réserve le droit d'interdire l'accès à tout membre du personnel de l'entrepreneur, à tout moment.

   Lorsque la GRC détermine qu'une autorisation d'accès à l'installation (FA2), une cote de fiabilité approfondie, ou une cote de fiabilité approfondie avec autorisation de niveau Secret est nécessaire, elle invite les entrepreneurs à visiter son portail en ligne pour y remplir les formulaires d'autorisation.

La GRC

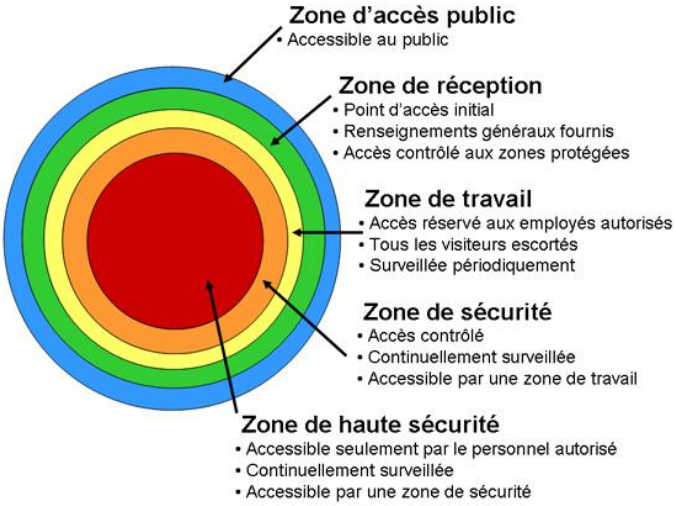
1. procédera à des vérifications de filtrage de sécurité du personnel dépassant les exigences de sécurité prescrites par la Politique sur la sécurité du gouvernement.

   La GRC se réserve le droit d'augmenter ou de modifier les niveaux de sécurité requis, selon ce qu'elle juge approprié, lorsque les rôles professionnels auront été mieux définis.

Annexe B – Concept de la zone de sécurité

La Politique sur la sécurité du gouvernement (section 10.8 – Limites à l'accès) stipule que « les ministères doivent limiter l'accès aux renseignements classifiés et protégés et autres biens aux seules personnes qui ont besoin de les connaître et qui ont la cote de fiabilité ou de sécurité appropriée ».

La Norme opérationnelle sur la sécurité matérielle stipule ce qui suit (section 6.2 – Hiérarchie des zones) : « Les ministères doivent assurer l'accès et la protection des biens protégés et classifiés en fonction d'une hiérarchie des zones clairement reconnaissable ».



La **zone d'accès public** est une zone où le public peut circuler librement et qui entoure habituellement un immeuble gouvernemental ou en fait partie. Il s'agit par exemple des terrains entourant un immeuble et des corridors publics, ainsi que des vestibules d'ascenseur dans les immeubles à plusieurs occupants.

La **zone de réception** est une zone où la transition d'une zone d'accès public à une zone à accès restreint est délimitée et contrôlée. Elle est généralement située à l'entrée de l'immeuble où survient le premier contact entre le public et le Ministère, y compris les endroits où des services sont fournis et où des renseignements sont échangés. L'accès du public peut être restreint pendant certaines heures de la journée ou pour des motifs particuliers.

La **zone de travail** est une zone dont l'accès est limité au personnel qui y travaille et aux visiteurs accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Il s'agit par exemple d'un espace à bureaux à aire ouverte typique ou du local des installations électriques type.

La **zone de sécurité** est une zone dont l'accès est limité au personnel autorisé ainsi qu'aux visiteurs autorisés et dûment accompagnés. Cette zone doit être délimitée par un périmètre reconnaissable et faire l'objet d'une surveillance continue, c'est-à-dire tous les jours, 24 heures sur 24. Il s'agit par exemple d'une zone où des renseignements secrets sont traités ou conservés.

La **zone de haute sécurité** est une zone dont l'accès est limité au personnel autorisé et détenant une cote de sécurité valide et de niveau approprié, ainsi qu'aux visiteurs autorisés et dûment accompagnés; elle doit être délimitée au moyen d'un périmètre construit selon les spécifications recommandées dans l'EMR et faire l'objet d'une surveillance continue, c'est-à-dire tous les jours, 24 heures sur 24. De plus, les renseignements concernant l'accès à cette zone doivent être enregistrés et vérifiés. Il s'agit par exemple d'une zone où des biens de grande valeur sont traités par des employés sélectionnés.

L'accès aux zones devrait reposer sur les principes du « besoin de savoir » et de la restriction de l'accès pour protéger les employés et les biens de valeur. Consulter le Guide G1-026 de la GRC, Guide pour l'établissement des zones de sécurité matérielle pour de plus amples détails.

ANNEXE D

Sécurité de la chaîne d'approvisionnement
Processus d'évaluation de l'information

a) **Exigence de qualification** : Pour devenir un Répondant qualifié et pouvoir soumissionner sur une demande de soumissions liée à ce processus d'approvisionnement, chaque Répondant provisoirement qualifié devra compléter avec succès l'évaluation préliminaire de l'intégrité de la chaîne d'approvisionnement (ICA) et ne doit pas être définitivement disqualifié. Une évaluation complète de l'ICA sera menée par le Canada au stade de la demande de propositions

b) **Définitions** : Les expressions et mots suivants, qui sont utilisés dans le cadre de l'évaluation préliminaire de l'ICA, ont la signification suivante :

a) **« Produit »** désigne tout matériel qui fonctionne dans la couche liaison de données du modèle d'interconnexion de systèmes ouverts (modèle OSI) de couche 2 ou supérieur; tout logiciel et tout appareil de technologie en milieu de travail;

b) **« Appareils technologiques en milieu de travail »** désigne les ordinateurs de bureau, les postes de travail mobiles (comme les ordinateurs portables ou les tablettes), les téléphones intelligents ou les téléphones, ainsi que les périphériques et les accessoires comme les moniteurs, les claviers, les souris, les dispositifs audio ou les dispositifs de stockage internes ou externes comme les clés USB, les cartes à mémoire, les disques durs externes ou les CD et DVD inscriptibles ou tout autre média;

c) **« Fabricant du produit »** désigne l'entité qui assemble les composants pour fabriquer le produit final;

d) **« Éditeur de logiciel »** : Propriétaire du logiciel qui a le droit d'octroyer une licence (et d'autoriser d'autres personnes à octroyer une licence ou une sous-licence) pour ses produits logiciels;

e) **« Données du Canada »** désigne toute donnée provenant des travaux, toute donnée reçue visant à contribuer aux travaux ou générée dans le cadre de la prestation de services de sécurité, de configuration, d'exploitation, d'administration et de gestion, ainsi que toute donnée transportée ou stockée par l'entrepreneur ou le sous-traitant dans le cadre des travaux en vertu de tout contrat découlant d'une demande de soumissions subséquente;

f) **« Travaux »** désigne les activités, services, biens, équipements, choses et objets que l'entrepreneur doit exécuter, livrer ou fournir en vertu de tout contrat découlant d'une demande de soumissions subséquente.

c) **Exigences de présentation pour l'évaluation préliminaire de l'ICA (partie de l'étape 2 de l'ISQ)**:

a) Les Répondants provisoirement qualifiés doivent soumettre les informations énumérées ci-dessous avant l'expiration d'une période de trois semaines à compter de la date du courriel envoyé par TPSGC directement aux Répondants provisoirement qualifiés demandant la soumission. Le Canada demande que les Répondants

provisoirement qualifiés fournissent les renseignements en utilisant le formulaire 5 - Informations sur la sécurité de la chaîne d'approvisionnement, mais la forme sous laquelle les renseignements sont soumis n'est pas en soi obligatoire. Le Canada demande également que, sur chaque page, les Répondants provisoirement qualifiés indiquent leur nom légal et insèrent un numéro de page ainsi que le nombre total de pages.

(A) **Informations sur la propriété des Répondants provisoirement qualifiés: Les Répondants provisoirement qualifiés doivent fournir pour l'évaluation préliminaire ICA:**

(1) Fournir les numéro Duns et Bradstreet des Répondants provisoirement qualifiés, ou :

(I) Informations sur la propriété : le Répondant provisoirement qualifié doit fournir une liste de tous ses actionnaires. Si le Répondant provisoirement qualifié est une filiale, cette information doit être fournie pour chaque société mère (personne morale ou société de personnes), et ce, jusqu'à l'ultime propriétaire. En ce qui concerne toute société cotée en bourse, le Répondant provisoirement qualifié doit inclure dans son offre une liste des actionnaires qui détiennent au moins 1 % des actions avec droit de vote ; toutefois, sur demande, un Répondant provisoirement qualifié coté en bourse doit fournir des renseignements supplémentaires sur les autres actionnaires;

(II) investisseurs qui ne sont pas des actionnaires;

(III) cadres supérieurs;

(IV) Conseil d'administration;

(2) Lien vers le site Web de l'entreprise.

(B) **Liste de produits du SGPN logiciel-service (SaaS) avec informations de localisation :** Les Répondants provisoirement qualifiés doivent dresser, pour l'ICA préliminaire, la liste des produits du SGPN logiciel-service (SaaS) qui pourraient servir à transmettre et à stocker les données du Canada, et qui pourraient être utilisés et installés par le Répondant provisoirement qualifié ou l'un de ses sous-traitants pour effectuer une partie des travaux, ainsi que les renseignements d'emplacement concernant chaque produit du SGPN logiciel-service (SaaS):

(1) Préciser où chaque produit SGPN logiciel-service (SaaS) est relié à un réseau donné pour ce qui est des données du Canada (définir les points ou les nœuds de prestation de services, comme les points de présence, les emplacements tiers, les installations des centres de données, les centres des opérations, les centres des opérations de sécurité, Internet ou tout autre point d'appairage du réseau public.);

(2) Le Canada demande aux Répondants provisoirement qualifiés d'insérer une ligne distincte à l'aide du formulaire 5 - Informations sur la sécurité de la chaîne d'approvisionnement pour chaque produit SGPN logiciel-service (SaaS). Le Canada demande également que les Répondants provisoirement qualifiés ne répètent pas plusieurs itérations du même produit (par exemple, si le numéro de série et / ou la couleur est la seule

différence entre deux produits SGPN logiciel-service (SaaS), ils seront traités comme le même SGPN logiciel-service (SaaS) aux fins de l'ICA préliminaire.

d) **Processus d'évaluation préliminaire de l'intégrité de la chaîne d'approvisionnement** :

a) Le Canada évaluera si la solution du Répondant provisoirement qualifié compromet ou sert à compromettre la sécurité du matériel, des micrologiciels, logiciels, systèmes ou renseignements lui appartenant.

b) Au cours de l'évaluation :

(A) Le gouvernement du Canada peut exiger du Répondant provisoirement qualifié des renseignements supplémentaires nécessaires pour effectuer une évaluation préliminaire complète de l'ICA. Le Répondant provisoirement qualifié disposera de deux jours ouvrables (ou d'une période plus longue si elle est précisée par écrit par l'autorité contractante) pour fournir les renseignements requis au gouvernement du Canada. À défaut de respecter ce délai, le Répondant provisoirement qualifié sera disqualifié.

(B) Le Canada peut confier l'évaluation à ses propres ressources ou à des experts-conseils et peut, au besoin, se procurer des renseignements supplémentaires auprès de tiers. Le Canada peut utiliser tout renseignement, qu'il se trouve dans la réponse ou qu'il provienne d'une autre source, qu'il juge utile afin d'effectuer une évaluation préliminaire de l'ICA.

c) Si le Canada juge qu'un aspect de l'ISCA, s'il est utilisé par le Canada, peut compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, logiciels, systèmes ou renseignements lui appartenant :

(A) Le gouvernement du Canada avisera le Répondant provisoirement qualifié par écrit (par courriel) et indiquera quel aspect de l'ISCA est préoccupant ou est impossible à évaluer (par exemple, des versions futures proposées de produits ne peuvent être évaluées). Tout autre renseignement que le Canada peut être en mesure de fournir au Répondant provisoirement qualifié concernant ses préoccupations sera déterminé selon sa nature. Dans certains cas, pour des raisons de sécurité nationale, il pourrait être impossible pour le Canada de fournir d'autres renseignements au Répondant provisoirement qualifié. Par conséquent, dans certaines circonstances, le Répondant provisoirement qualifié ne connaîtra pas les raisons sous-jacentes des préoccupations du Canada relativement au produit, au sous-traitant ou à d'autres aspects de l'ISCA. En ce qui concerne les préoccupations éventuelles, le Canada peut, à son entière discrétion, déterminer une éventuelle mesure d'atténuation que le Répondant provisoirement qualifié pourrait devoir mettre en œuvre par rapport à n'importe quelle portion de l'ISCA si un contrat lui est attribué.

(B) Après réception de l'avis écrit du Canada, le Répondant provisoirement qualifié pourra présenter l'ISCA modifiée dans un délai de 10 jours civils (ou à l'intérieur d'un délai plus long précisé par écrit par l'autorité contractante). Si le Canada a déterminé une mesure d'atténuation que le fournisseur pourrait devoir mettre en œuvre si un contrat lui est attribué, le Répondant provisoirement qualifié doit confirmer dans sa soumission de l'ISCA révisée son consentement ou son refus que toutes condition dans l'EAB ou DDP ou contrat attribué comprenne des engagements supplémentaires relatifs à ces conditions d'atténuation.

(C) Si le Répondant provisoirement qualifié présente l'ISCA révisée dans le délai imparti, le Canada procédera à une deuxième évaluation. Si le Canada juge que l'ISCA révisée du Répondant provisoirement qualifié pourrait compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, logiciels, systèmes ou renseignements lui appartenant, il n'offrira pas au Répondant provisoirement qualifié d'autre occasion de réviser l'ISCA; le Répondant provisoirement qualifié ne sera pas retenu et ne sera pas en mesure de participer aux étapes subséquentes du processus d'approvisionnement. Si l'approbation du Canada est visée par toute mesure d'atténuation, aucun contrat ne sera attribué au Répondant provisoirement qualifié et le Répondant provisoirement qualifié ne pourra pas participer au reste du processus d'approvisionnement, à moins que le Canada soit convaincu que le contrat comprend des engagements additionnels reflétant les mesures d'atténuation requises.

d) En participant à ce processus, le Répondant provisoirement qualifié reconnaît que la nature de la technologie de l'information est constamment exposée à de nouvelles brèches, y compris des brèches en matière de sécurité. En outre, le Répondant provisoirement qualifié reconnaît que l'évaluation de sécurité du Canada ne couvre pas l'évaluation d'une éventuelle solution. Par conséquent :

(A) une qualification dans le cadre de cette évaluation préliminaire de l'ICA ne constitue pas une reconnaissance que les produits ou d'autres renseignements inclus dans l'ICA préliminaire satisfont aux exigences d'une demande de propositions subséquente ou de tout contrat en découlant ou de tout autre instrument pouvant être attribué à la suite d'une demande de soumissions subséquente y compris l'éventuelle DDP, le cas échéant, dans cet approvisionnement;

(B) une qualification à la présente ISQ à la suite de l'évaluation préliminaire de l'ICA ne signifie pas que de l'information identique ou semblable sur la sécurité de la chaîne d'approvisionnement sera évaluée de la même façon pour de futurs besoins;

(C) à tout moment durant les prochaines étapes de ce processus d'approvisionnement, le Canada peut aviser le Répondant qualifié que certains aspects de son ISCA soulèvent des préoccupations en matière de sécurité. Le cas échéant, le Canada avisera le Répondant qualifié et lui donnera l'occasion de réviser ses renseignements sur l'ISCA suivant le processus décrit ci-dessus; et

(D) Au cours de l'exécution d'un contrat découlant d'une demande de propositions subséquente, si le Canada est préoccupé par certains produits, concepts et sous-traitants initialement visés par l'ISCA, il traitera la situation conformément aux modalités du contrat.

e) Tous les Répondant provisoirement qualifié seront avisés par un avis écrit, qui leur indiquera s'ils se sont qualifiés ou non dans le cadre de l'évaluation préliminaire de l'ICA.

f) Tout Répondant provisoirement qualifié dans le cadre de l'évaluation préliminaire de l'ICA devra, dans sa réponse à une demande de propositions subséquente de ce processus d'approvisionnement, proposer une chaine d'approvisionnement cohérente avec l'information sur la sécurité de la chaîne d'approvisionnement soumise dans le cadre de l'ICA préliminaire, en particulier avec l'ISCA soumis en réponse aux informations de propriété pour les Répondants provisoirement qualifiés dans la sous-section c) (a) (A) et la

liste de produits SGPN logiciel-service (SaaS) avec des informations de localisation dans la sous-section c) (a) (B) de ce document (sujet à la révision uniquement conformément au prochain sous-article). Sauf conformément au paragraphe ci-dessous, aucune information alternative ou supplémentaire soumise en vertu du paragraphe c) (a) (A) ou c) (a) (B) ne peut être proposée à l'étape de la DP.

g) Une fois qu'un Répondant provisoirement qualifié est qualifié suite à l'évaluation préliminaire de l'ICA, il ne sera pas permis d'apporter de modifications aux renseignements sur la sécurité de la chaîne d'approvisionnement, sauf dans certaines situations exceptionnelles, que détermine le Canada. Comme il n'est pas possible de prévoir toutes les circonstances exceptionnelles, le Canada, pour chacun des cas qui se présentent, déterminera si des modifications sont permises et définira le processus régissant ces modifications.

h) En soumettant son ICA pour évaluation préliminaire et dans l'esprit de participation au présent processus d'approvisionnement, le Répondant provisoirement qualifié accepte les modalités de l'entente de non-divulgation ci-dessous (« **entente de non-divulgation** ») :

a) Le Répondant provisoirement qualifié accepte d'assurer la confidentialité de toute information qu'il reçoit du Canada au sujet de l'évaluation qu'a faite ce dernier de l'information sur la sécurité de la chaîne d'approvisionnement fournie par le Répondant provisoirement qualifié (« **l'information sensible** »), notamment en ce qui touche les aspects de l'information sur la chaîne de sécurité qui soulèvent des préoccupations et les raisons derrière ces préoccupations du Canada.

b) Le Répondant provisoirement qualifié accepte également de conserver l'information en question en lieu sûr. L'information sensible comprend, notamment, les documents, les instructions, les directives, les données, le matériel, les conseils ou autre renseignement, quels qu'ils soient, fournis verbalement, par écrit ou autrement, et ce, peu importe que cette information soit classifiée, confidentielle, exclusive ou sensible.

c) Le Répondant provisoirement qualifié convient de ne pas reproduire, copier, divulguer, publier ou communiquer, en tout ou en partie et de quelque façon que ce soit, de l'information sensible à une personne autre qu'un employé du Répondant provisoirement qualifié ayant besoin de connaître l'information et détenant une cote de sécurité correspondant à la sensibilité de l'information divulguée, sans le consentement écrit préalable de l'autorité contractante.

d) Le Répondant provisoirement qualifié accepte d'aviser immédiatement l'autorité contractante dès qu'une personne autre que celles autorisées en vertu du précédent article accède à de l'information sensible.

e) Le Répondant provisoirement qualifié comprend et accepte le fait que le non-respect de cette entente de non-divulgation peut entraîner sa disqualification à tout moment pendant le processus d'approvisionnement, voire la résiliation immédiate d'un contrat ou autre instrument subséquent. Le Répondant provisoirement qualifié reconnaît également que toute violation de cette entente de non-divulgation peut entraîner un examen de sa cote de sécurité et de son statut de soumissionnaire admissible dans l'éventualité d'autres besoins.

f) Toute l'information sensible demeurera la propriété du Canada et doit être retournée à l'autorité contractante ou détruite à la demande de cette dernière, dans les 30 jours suivant cette demande.

g) La présente entente de non-divulgation demeure en vigueur indéfiniment. Si le Répondant provisoirement qualifié souhaite être dégagé de ses obligations qu'impose tout document comprenant de l'information sensible, il peut retourner toute la documentation visée au représentant adéquat du Canada, en faisant mention de la présente entente de non-divulgation. Dans ce cas, toute l'information sensible connue du Répondant provisoirement qualifié et de son personnel (information sensible connue, mais non écrite) demeure encadrée par la présente entente de non-divulgation, mais le Répondant provisoirement qualifié n'a plus l'obligation de ranger dans un endroit sûr les documents contenant cette information sensible (sauf s'il a créé de nouveaux documents contenant de l'information sensible. Le Canada pourrait exiger du Répondant provisoirement qualifié qu'il fournisse une confirmation écrite que toutes les copies papier et électroniques des documents qui comprennent de l'information sensible ont été rendues au gouvernement du Canada.

f) **Exigences de soumission anticipées pour l'évaluation complète de l'ICA (les fournisseurs qualifiés seront informés des exigences à l'étape de la demande de propositions) - Fournies uniquement à des fins d'information à cette étape de l'ISQ:**

Veuillez noter qu'à l'avenir, sous réserve de modifications possibles, le Canada exigera probablement les informations suivantes:

(A) **Liste complète des produits (Caméras Corporelles):**

(1) Emplacement : Préciser où chaque produit est relié à un réseau donné pour ce qui est des données du Canada (définir les points ou les nœuds de prestation de services, comme les points de présence, les emplacements tiers, les installations des centres de données, les centres des opérations, les centres des opérations de sécurité, Internet ou tout autre point d'appairage du réseau public.);

(2) **Type de produit** : Énoncer la description généralement reconnue utilisée par l'industrie pour le matériel ou les logiciels, etc. Les composantes d'un produit assemblé, comme un module ou un assemblage de cartes, doivent être fournies pour tous les appareils d'interconnexion de réseaux de la troisième couche;

(3) **Composant**: indiquer la description généralement reconnue par l'industrie pour les coupe-feu, routeurs, interrupteurs, serveurs, applications de sécurité, etc.;

(4) **Nom ou numéro du modèle de produit** : Préciser le nom ou le numéro annoncé du produit par lequel le fabricant désigne son produit;

(5) **Description et fonction du produit** : préciser la description ou la fonction annoncée par le fabricant du produit et l'utilisation ou le rôle prévu dans les travaux décrits dans le projet;

(6) **Source** : Préciser le nom du fabricant du produit et/ou de l'éditeur de logiciels des composants intégrés;

(7) **Nom du sous-traitant** : indiquer tous les sous-traitants. Dans le formulaire d'ISCA joint à la présente ISQ, le nom du sous-traitant renvoie à tout sous-traitant qui fournira, installera ou entretiendra au moins un produit, si le Répondant ne le fait pas lui-même, comme il est décrit ci-dessous.

(B) **Liste complète des produits (SGPN logiciel-service - SaaS)**

(1) Emplacement : Préciser où chaque produit est relié à un réseau donné pour ce qui est des données du Canada (définir les points ou les nœuds de prestation de services, comme les points de présence, les emplacements tiers, les installations des centres de données, les centres des opérations, les centres des opérations de sécurité, Internet ou tout autre point d'appairage du réseau public.);

(2) **Type de produit** : Énoncer la description généralement reconnue utilisée par l'industrie pour le matériel ou les logiciels, etc. Les composantes d'un produit assemblé, comme un module ou un assemblage de cartes, doivent être fournies pour tous les appareils d'interconnexion de réseaux de la troisième couche;

(3) **Composant**: indiquer la description généralement reconnue par l'industrie pour les coupe-feu, routeurs, interrupteurs, serveurs, applications de sécurité, etc.;

(4) **Nom ou numéro du modèle de produit** : Préciser le nom ou le numéro annoncé du produit par lequel le fabricant désigne son produit;

(5) **Description et fonction du produit** : préciser la description ou la fonction annoncée par le fabricant du produit et l'utilisation ou le rôle prévu dans les travaux décrits dans le projet;

(6) **Source** : Préciser le nom du fabricant du produit et/ou de l'éditeur de logiciels des composants intégrés;

(7) **Nom du sous-traitant** : indiquer tous les sous-traitants. Dans le formulaire d'ISCA joint à la présente ISQ, le nom du sous-traitant renvoie à tout sous-traitant qui fournira, installera ou entretiendra au moins un produit, si le Répondant ne le fait pas lui-même, comme il est décrit ci-dessous.

(C) **Diagrammes de réseau** : un ou plus de un diagramme de réseau conceptuel montrant ensemble la totalité du réseau proposé pour l'exécution des travaux décrits dans la présente ISQ. Les diagrammes de réseau doivent uniquement comprendre les portions du réseau du Répondant provisoirement qualifié (et de ceux de ses sous-traitants) sur lequel des données du Canada seraient transmises dans l'exécution du contrat subséquent. Probablement, à tout le moins, le diagramme doit illustrer ce qui suit :

(1) les principaux nœuds suivants servant à la prestation de services dans le cadre de tout contrat subséquent :

(I) points de prestation de service;

(II) réseau de base;

(III) les réseaux du sous-traitant (préciser le nom du sous-traitant qui figure sur la liste des sous-traitants);

(2) les interconnexions entre les nœuds, s'il y a lieu;

(3) toute interconnexion entre les nœuds et Internet;

(4) pour chaque nœud, un renvoi au produit qui sera déployé dans ce nœud, à l'aide du numéro d'article de la liste des produits de TI.

(D) **Liste des sous-traitants:** une liste de tous les sous-traitants qui pourraient être utilisés pour exécuter toute partie des travaux (y compris les sous-traitants affiliés ou autrement liés au soumissionnaire) conformément à tout contrat subséquent. La liste doit comprendre au minimum:

(1) le nom du sous-traitant;

(2) l'adresse du siège du sous-traitant;

(3) la partie des travaux qui serait exécutée par le sous-traitant; et

(4) le (s) endroit (s) où le sous-traitant exécuterait les travaux.

Cette liste doit identifier tous les tiers qui peuvent exécuter toute partie des travaux, qu'il s'agisse de sous-traitants du soumissionnaire ou de sous-traitants de sous-traitants du soumissionnaire en aval de la chaîne. Cela signifie que chaque sous-traitant qui pourrait avoir accès aux données du Canada ou qui serait responsable de leur transport ou de leur stockage doit être identifié. Les sous-traitants comprendraient également, par exemple, des techniciens qui pourraient être déployés pour maintenir la solution du soumissionnaire. Aux fins de cette exigence, un tiers qui est simplement un fournisseur de biens pour le soumissionnaire, mais qui n'exécute aucune partie des travaux, n'est pas considéré comme un sous-traitant. Si le soumissionnaire ne prévoit pas faire appel à des sous-traitants pour exécuter une partie des travaux, le Canada demande que le soumissionnaire l'indique dans sa réponse.

ANNEXE E

POLITIQUES, LOIS ET RENSEIGNEMENTS CLÉS

Cette section est fournie à titre informatif uniquement à ce stade. Elle met en évidence certaines des diverses politiques et lois qui pourraient devoir être prises en considération tant pour la demande de propositions que pour le contrat subséquent. Notez que la liste peut ne pas être complète et que d'autres politiques et lois pourraient également s'appliquer.

1. Normes et politique numériques

a) Les normes numériques du gouvernement du Canada (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/normes-numeriques-gouvernement-canada.html) constituent le fondement du virage du gouvernement vers une plus grande souplesse, une plus grande ouverture et une plus grande attention sur l'utilisateur. Elles guideront les équipes dans la conception de services numériques, d'une façon qui servira le mieux les Canadiens.

b) La Politique sur les services et le numérique (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603) constitue un ensemble intégré de règles qui décrit la façon dont les organisations du gouvernement du Canada gèrent la prestation de services, l'information et les données, la technologie de l'information et la cybersécurité à l'ère du numérique.

2. Normes d'interopérabilité

Normes du gouvernement du Canada sur les interfaces de programmation d'applications (API) (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html) – Ces normes régissent la façon dont les API doivent être élaborées à l'échelle du GC afin de mieux appuyer les processus numériques intégrés dans l'ensemble des ministères et des organismes.

3. Infonuagique et souveraineté des données

Gouvernement du Canada Livre blanc : Souveraineté des données et nuage public (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/gc-livre-blanc-souverainete-donnees-nuage-public.html) – Ce document vise à donner un aperçu du risque pour la souveraineté des données, ainsi que du risque pour l'emplacement des données et la sécurité des données, qui ont trait à l'utilisation de services d'informatique en nuage publics commerciaux. On examine ces risques dans le contexte de la stratégie « Le nuage d'abord » du GC. À la fin du document, le lecteur comprendra les risques et les mesures d'atténuation qui s'appliquent. Le lecteur comprendra également en quoi les services d'informatique en nuage peuvent aider le GC à gérer d'autres risques, notamment : vieillissement de la TI, lacunes actuelles en matière de sécurité, et manquement à bénéficier des technologies émergentes.

4. Protection de la vie privée

a) Politique intérimaire sur la protection de la vie privée (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510) – Les objectifs de cette politique intérimaire sont les suivants : faciliter la

conformité législative et réglementaire, ainsi que renforcer l'application efficace de la *Loi sur la protection des renseignements personnels* et de son Règlement par les institutions fédérales; assurer l'application uniforme de pratiques et procédures dans l'administration de la Loi et du Règlement; et assurer la protection et la gestion efficace des renseignements personnels et atténuer les risques d'entrave à la vie privée dans les programmes et activités du gouvernement.

b) *Loi sur l'accès à l'information* https://laws.justice.gc.ca/fra/lois/A-1/index.html – Loi visant à compléter la législation canadienne en matière d'accès à l'information relevant du gouvernement du Canada.

c) *Loi sur la protection des renseignements personnels* (https://laws.justice.gc.ca/fra/lois/P-21/index.html) – Loi visant à compléter la législation canadienne en matière de protection des renseignements personnels et de droit d'accès des individus aux renseignements personnels qui les concernent.

5. Politique en matière de sécurité

Politique sur la sécurité du gouvernement (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578) – Fournit une orientation sur la gestion de la sécurité du gouvernement à l'appui de l'exécution des programmes et de la prestation des services fiables du GC ainsi que de la protection des renseignements, des particuliers et des biens, et donne à la population canadienne, aux partenaires, aux organismes de surveillance et aux autres intervenants une assurance au regard de la gestion de la sécurité au sein du GC.

6. Accessibilité

a) Norme sur l'accessibilité des sites Web (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601) : le but de cette norme est d'assurer un haut niveau d'accessibilité Web, appliquée uniformément à l'ensemble des sites Web et applications Web du gouvernement du Canada.

b) Stratégie sur l'accessibilité au sein de la fonction publique du Canada – (https://www.canada.ca/fr/gouvernement/fonctionpublique/mieux-etre-inclusion-diversite-fonction-publique/diversite-equite-matiere-emploi/accessibilite-fonction-publique/strategie-accessibilite-fonction-publique-tdm.html) – La stratégie décrit comment la vision du GC de devenir la fonction publique la plus accessible et la plus inclusive au monde et comment les principes directeurs de « Rien sans nous », de collaboration, de durabilité et de transparence doivent être mis en œuvre.

c) *Loi canadienne sur l'accessibilité* (https://www.parl.ca/DocumentViewer/fr/42-1/projet-loi/C-81/sanction-royal) – Cette loi a été promulguée afin de favoriser la participation pleine et égale dans la société de toutes les personnes, en particulier les personnes handicapées. La Loi vise à parvenir à cette fin par la transformation du Canada, dans le champ de compétence législative de Parlement, en un pays exempt d'obstacles, particulièrement par la reconnaissance, l'élimination et la prévention d'obstacles.

d) Règles pour l'accessibilité des contenus Web (https://www.w3.org/TR/WCAG21/) – Les Règles pour l'accessibilité des contenus Web (WCAG) 2.1 couvrent un large éventail de recommandations pour rendre les contenus Web plus accessibles. Le respect de ces lignes directrices rendra le contenu plus accessible à un nombre plus élevé de personnes en situation de handicap, y compris les adaptations pour la cécité et la basse vision, la surdité et la perte d'audition, les mouvements limités, les troubles de la parole, la photosensibilité et des combinaisons de ces éléments, et certaines adaptations pour les troubles d'apprentissage et les limitations cognitives; mais il ne répondra pas à tous les besoins des utilisateurs pour les

personnes ayant ces handicaps. Ces directives concernent l'accessibilité au contenu Web sur les ordinateurs de bureau, les ordinateurs portables, les tablettes et les appareils mobiles.

e) Ligne directrice sur l'utilisabilité de la technologie de l'information (TI) par tous (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32620) – Cette ligne directrice appuie l'orientation du gouvernement du Canada visant à garantir que les ministères, organismes et organisations tiennent compte de l'accessibilité lors de l'acquisition ou du développement de solutions et d'équipements de technologie de l'information (TU) afin de rendre les TI utilisables par tous.

7. Politique sur les langues officielles

La *Loi sur les langues officielles* (LLO) (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26160) réaffirme l'égalité de statut du français et de l'anglais à titre de langues officielles du Canada et indique que les deux langues officielles ont des droits et des privilèges égaux quant à leur usage dans les institutions. Cette politique a pour objectif d'aider les institutions à se conformer à la LLO et à son règlement d'application, et de faciliter l'application efficace de celle-ci.

8. Région du Nunavut

La Directive sur les marchés de l'État, incluant les baux immobiliers, dans la région du Nunavut (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32610) permet d'assurer que la passation des marchés de l'État dans la région du Nunavut respectera les obligations du gouvernement du Canada prévues par l'article 24 de l'Accord du Nunavut.

9. Ententes sur les revendications territoriales globales

Les traités modernes, aussi connus sous le nom d'ententes sur les revendications territoriales globales (ERTG), (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-approvisionnements/section/9/35) sont généralement tripartites et comprennent des organisations ou des nations autochtones, la Couronne et les gouvernements provinciaux et territoriaux comme signataires. Elles apportent clarté et prévisibilité en ce qui concerne les droits sur les terres et les ressources, la propriété et la gestion. Les traités modernes/ERTG visent également à assurer un traitement équitable des intérêts autochtones en ce qui concerne les droits culturels, sociaux, politiques et économiques, y compris les droits à la terre, à la pêche, à la chasse et à la pratique de leur propre culture. Les droits qui y sont définis sont protégés par l'article 35 de la *Loi constitutionnelle*, 1982.

FORMULAIRE 1 – FORMULAIRE DE DÉCLARATION DU RÉPONDANT ET DE PRÉSENTATION DE LA RÉPONSE

En présentant sa réponse, le Répondant garantit au Canada que les renseignements ci-dessous sont exacts.

1. Dénomination sociale complète du Répondant Le terme « Répondant » désigne la personne ou l'entité qui présente la réponse. Les Répondants qui font partie d'un groupe de sociétés devraient identifier clairement la société qui est la véritable Répondante.	
Nom	[DÉNOMINATION SOCIALE COMPLÈTE DU RÉPONDANT]
Dénomination commerciale, si elle est différente de la dénomination sociale	
Adresse postale	[ADRESSE COMPLÈTE DU RÉPONDANT INCLUANT: Numéro/nom de rue, numéro d'unité/de bureau/d'appartement Ville, province, territoire Code postal Pays]
Adresse civique (physique)	[ADRESSE COMPLÈTE DU RÉPONDANT INCLUANT: Numéro/nom de rue, numéro d'unité/de bureau/d'appartement Ville, province, territoire Code postal Pays]
Numéro de téléphone de l'organisation	
2. Numéro d'entreprise – approvisionnement (NEA) du Répondant [Remarque à l'intention des Répondants : Le NEA donné doit correspondre à la dénomination sociale utilisée dans la réponse. Si ce n'est pas le cas, on établira le Répondant en fonction de la dénomination sociale fournie, et le Répondant devra fournir le NEA qui correspond à cette dernière.]	
Numéro d'entreprise - approvisionnement	[NUMÉRO D'ENTREPRISE – APPROVISIONNEMENT]
3. Représentant autorisé du Répondant	
Nom	
Titre	

Numéro de téléphone au travail	
Numéro de téléphone cellulaire	
Courriel	

4. Identification de toutes les parties de la coentreprise
Si la réponse est présentée pour le compte d'une coentreprise, le Répondant doit fournir l'information; autrement, inscrire « s. o. ».

Noms des personnes ou entités membres de la coentreprise	**NEA de chaque membre de la coentreprise**

5. Langue de préférence	S'il est qualifié pour participer à la prochaine étape du processus d'approvisionnement, le Répondant préférerait recevoir la correspondance et les documents d'approvisionnement connexes dans la langue suivante : Anglais □ Français □
6. Programme de contrats fédéraux pour l'équité en matière d'emploi	
Admissibilité à répondre Programme de contrats fédéraux pour l'équité en matière d'emploi	[ ] Le Répondant et toutes ses personnes et entités membres s'il s'agit d'une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée » du Programme de contrats fédéraux pour l'équité en matière d'emploi. *Le Canada aura le droit de déclarer une réponse non recevable si le Répondant, ou toute personne ou entité membre de la coentreprise si le soumissionnaire est une coentreprise, figure sur la liste des soumissionnaires à admissibilité limitée du PCF au moment de l'attribution du contrat.*
7. Code de conduite pour l'approvisionnement	[ ] Le Répondant se conforme au Code de conduite pour l'approvisionnement du Canada (le « Code »).
8. Politique d'inadmissibilité et de suspension	[ ] Le Répondant a lu et compris les exigences de la Politique d'inadmissibilité et de suspension du Canada (la « Politique ») et les directives applicables en vigueur à la date de publication de la demande de soumissions et s'y conforme. [ ] Le Répondant n'est pas actuellement suspendu ni inadmissible aux termes de la Politique. [ ] Le Répondant comprend que toute accusation ou condamnation criminelle ultérieure peut entraîner sa suspension ou son inadmissibilité à conclure des contrats avec le Canada.

Liste des membres du conseil d'administration *(Prénom et nom de famille)*
La liste peut être jointe à la présente annexe
Autres membres *(prénom et nom de famille)*

1. Directeur	
2. Directeur	
3. Directeur	
4. Directeur	
5. Directeur	
6. Directeur	
7. Directeur	
8. Directeur	
9. Directeur	
10. Directeur	
[Insérer le titre]	
[Insérer le titre]	
9. Exigences en matière d'accessibilité (tel qu'indiqué au critère O7 de la pièce jointe 5.1 des critères d'évaluation obligatoires)	[ ] Le Répondant a lu et comprend les exigences en matière d'accessibilité telles qu'elles sont décrites dans les Règles pour l'accessibilité des contenus Web (WCAG) 2.0, conformément à la Norme sur l'accessibilité des sites Web du Canada et la Stratégie d'accessibilité pour la fonction publique du Canada. Oui ☐ Non ☐
10. Exactitude et intégrité Exactitude des renseignements	[ ] Tous les renseignements que le Répondant transmet avec sa réponse sont vrais, exacts et complets à la date indiquée ci-dessous.

11. Déclaration et signatures

Le Répondant déclare que la personne nommée ci-après à titre de représentant du Répondant détient tous les pouvoirs nécessaires pour le représenter dans le cadre de tous les éléments liés à sa réponse, y compris le pouvoir de donner des précisions et des renseignements supplémentaires qui pourraient être demandés à ce titre.

Le Répondant reconnaît aussi par les présentes ce qui suit :
a. Le présent formulaire de déclaration de réponse a été dûment autorisé et signé;
b. Le Répondant a reçu, lu, examiné, compris le formulaire et accepte d'être lié par toute l'invitation à se qualifier, y compris toutes les modifications s'y rapportant;
c. Le Répondant est lié par toutes les déclarations et tous les énoncés qu'il a faits dans sa réponse à l'invitation à se qualifier;
d. Le Répondant reconnaît que les renseignements fournis ci-dessus seront utilisés pour étayer l'évaluation de sa réponse.

Je, soussigné, à titre de mandant du Répondant, atteste par la présente que les renseignements fournis dans le présent formulaire et dans la réponse présentée sont exacts, à ma connaissance, et que j'ai le pouvoir d'assujettir la société/le partenariat/l'entreprise à propriétaire unique/la coentreprise.

Nom et titre du représentant autorisé à signer au nom du Répondant	_____ Nom du représentant autorisé _____ Titre du représentant autorisé
Signature du représentant autorisé à signer au nom du Répondant et date de la	

signature	_____ Signature du représentant autorisé Date

FORMULAIRE 2 – FORMULAIRE DE VÉRIFICATION DES PROJETS CITÉS EN RÉFÉRENCE

Instructions à l'intention des Répondants

(a) Les soumissionnaires doivent soumettre un formulaire de vérification des projets cités en référence pour chaque projet mentionné en réponse à chaque exigence obligatoire de l'annexe B – Critères d'évaluation obligatoires de l'ISQ.

(b) Si les renseignements demandés dans ce formulaire n'accompagnent pas la réponse à l'IQ du Répondant, celui-ci doit fournir lesdits renseignements à la demande de l'autorité contractante dans le délai précisé dans la demande.

(c) Le Canada peut communiquer avec la personne-ressource du client, indiquée pour le projet cité en référence, afin de valider les renseignements fournis.

#	Réponse
(a)	Numéro de l'exigence obligatoire (de l'annexe B – Critères d'évaluation obligatoires)
(b)	Dénomination sociale du Répondant (si le Répondant est constitué en coentreprise, la dénomination sociale du membre de la coentreprise pour le projet cité en référence)
(c)	Description du projet cité en référence
(d)	Nom de l'organisation d'application de la loi (le projet cité en référence)
(e)	Nom de la personne-ressource qui est responsable d'accepter la livraison des services pour le projet cité en référence
(f)	Titre de la personne-ressource
(g)	Numéro de téléphone actuel de la personne-ressource
(h)	Adresse courriel actuelle de la personne-ressource
(i)	Rôle et responsabilité de la personne-ressource du client dans le cadre du projet cité en référence

FORMULAIRE 3 – FORMULAIRE D'ATTESTATION DE L'ÉDITEUR DE LOGICIELS-SERVICES

Le Répondant _____ [insérer le nom du partenaire de la coentreprise, le cas échéant] atteste qu'il est l'éditeur du logiciel-service de la solution de Système de gestion de preuves numériques (SGPN) proposée et qu'il a tous les droits requis pour octroyer des licences et fournir des logiciels-services au Canada conformément au critère O4 de l'annexe B.

Nom de la solution de SGPN : _____

Nom de l'éditeur du logiciel-service : _____

Signature du signataire autorisé de l'éditeur du logiciel-service :_____

Titre en caractère d'imprimerie du signataire autorisé de l'éditeur du logiciel-service :_____

Adresse du signataire autorisé de l'éditeur du logiciel-service : _____

No de téléphone du signataire autorisé de l'éditeur du logiciel-service : _____

Courriel du signataire autorisé de l'éditeur du logiciel-service : _____

Date de signature : _____

Numéro de l'ISQ : _____

FORMULAIRE 4 – FORMULAIRE D'AUTORISATION DU FOURNISSEUR DE SERVICES INFONUAGIQUES DU GOUVERNEMENT DU CANADA

Le fournisseur de services infonuagiques (FSI) du Canada (GC) identifié ci-dessous reconnaît que le Répondant nommé ci-dessous a soumis une réponse à l'invitation à se qualifier (ISQ) (numéro de référence M7594-212120/F) conformément au critère obligatoire O8 de l'annexe B, pour une solution proposée de Système de gestion de preuves numériques (SGPN) à déployer sur le nuage approuvé par le GC et identifié ci-dessous.

Le FSI GC confirme que :

(i) Le fournisseur nommé ci-dessous est autorisé à déployer sa solution de SGPN sur le nuage identifié ci-dessous.

(ii) Le nuage identifié ci-dessous sur lequel la solution de SGPN proposée doit être déployée et hébergée répond au Profil de contrôle de sécurité pour les services GC fondés sur l'informatique en nuage. (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html).

Nom de la solution de SGPN :_____

Nom du nuage approuvé par le GC :_____

Nom du Répondant : _____

Nom du GC CSP :_____

Signature du signataire autorisé du FSI GC :_____

Titre en caractère d'imprimerie du signataire autorisé du FSI GC :_____

Adresse du signataire autorisé du FSI GC : _____

No de téléphone du signataire autorisé du FSI GC :_____

Courriel du signataire autorisé du FSI GC :_____

Date de signature :_____

FORMULAIRE 5: INFORMATIONS SUR LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT (ISCA)

Le formulaire est disponible sur demande à l'adresse courriel suivante:

Autorité Contractante
Nom: Kent Cummings
Travaux publics et Services gouvernementaux Canada

Adresse du courriel : TPSGC.PACCSGPN-APBWCDEMS.PWGSC@tpsgc-pwgsc.gc.ca