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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Par courriel à:
TPSGC.PACCSGPN-APBWCDEMS.PWGSC@tpsgc-pwgsc.gc.ca
Veuillez vous référer à la DDR

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Special Projects Division (SPD)/Division de Projets Spéciaux (DPS)
Terrasses de la Chaudière 4th Floo
Terrasses de la Chaudière 4e étage
10 Wellington Street,
10 Wellington Street,
Gatineau
Québec
K1A 0S5

Title - Sujet DDR#003 SGPN/Caméras corporelles	
Solicitation No. - N° de l'invitation M7594-212120/D	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client M7594-212120	**Date** 2021-04-06
GETS Reference No. - N° de référence de SEAG PW-$$XU-005-39339	
File No. - N° de dossier 005xu.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 2021-04-13 Heure Avancée de l'Est HAE

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

Address Enquiries to: - Adresser toutes questions à: Mulligan, Kate	**Buyer Id - Id de l'acheteur** 005xu
Telephone No. - N° de téléphone (873) 353-9579 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
Gendarmerie Royale du Canada
1200 Promenade Vanier
Ottawa, ON K1A 0R2

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

Signature **Date**

Canada

Demande de renseignements n° M7594-212120/D

Système de gestion de preuves numériques national (SGPN)

et caméras corporelles

MODIFICATION N° 001

La présente modification à la demande de renseignements (DDR) vise à :

1. Prolonger la date de clôture de la DDR, et
2. Fournir à l'industrie l'annexe A - Aperçu et description de haut niveau du besoin provisoires;

La demande de renseignements est modifiée par la présente comme suit :

1. À la page 1 de 1 de la DDR :

SUPPRIMER ce qui suit:

Solicitation Closes – L'invitation prend fin
At – à 02:00 PM
On – le 2021-04-09

INSÉRER la suivante pour la remplacer :

Solicitation Closes – L'invitation prend fin
At – à 02:00 PM
On – le 2021-04-13

2. À la page 9 de la DDR :

SUPPRIMER l'annexe A - Aperçu et description de haut niveau du besoin provisoires en totalité et **INSÉRER** l'annexe A - Aperçu et description de haut niveau du besoin provisoires ci-attaché pour le remplacer :

TOUTES LES AUTRES MODALITÉS DEMEURENT INCHANGÉES.

ANNEXE A

APERÇU ET DESCRIPTION DE HAUT NIVEAU DU BESOIN PROVISOIRES

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, provinciale, territoriale et fédérale. Elle fournit des services de police fédéraux, provinciaux, territoriaux et municipaux à la population canadienne dans 10 provinces, 3 territoires, 150 municipalités et plus de 600 communautés autochtones, notamment des services de police fédéraux et spécialisés fournis en soutien à des centaines d'autres organismes de sécurité publique et services de police du pays.

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 normaliser l'utilisation de caméras corporelles et d'un système de gestion de preuves numériques (SGPN) à l'échelle nationale pour tous les policiers de première ligne et aux services généraux au pays, soit entre 10 000 et 15 000 policiers, dont un grand nombre travaillent en milieu rural et isolé, dans environ 750 détachements au pays.

2. Principal motif de changement

2.1 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 caméras corporelles pour les policiers de la GRC. Bien qu'elle ne représente pas une panacée, l'utilisation de 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.

3. Utilisation de caméras corporelles

3.1 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.

3.2 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.

3.3 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. Les renseignements issus de ce projet pilote serviront à améliorer la politique opérationnelle, les procédures et les programmes de formation qui viennent appuyer le projet national de caméras corporelles et du SGPN.

3.4 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.

4. Objectifs et résultats opérationnels

4.1 La GRC cherche à obtenir les services d'un entrepreneur pour appuyer le déploiement national de caméras corporelles et la mise en œuvre d'un système de gestion des preuves numériques, dont il sera question plus en détail aux points 5.4.1 et 5.4.2. Nous avons pour objectif de trouver un entrepreneur d'ici l'été 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.

4.2 Grâce à la mise en œuvre d'un programme national de caméras corporelles 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.

4.3 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.

5. Portée fonctionnelle

5.1 L'entrepreneur choisi parmi les fournisseurs qualifiés devra fournir une solution permettant de livrer des caméras corporelles et un SGPN (matériel et logiciel) sous la forme d'un service entièrement géré et il aura la responsabilité globale de la mise en œuvre et des opérations de cette solution intégrée de caméras corporelles et de SGPN.

5.2 Cette solution devra pouvoir s'adapter aux exigences uniques de la GRC, répondre aux besoins

de la GRC en milieu urbain et rural, et fournir une capacité de solution dans plusieurs territoires de compétence, y compris dans les régions éloignées. La solution devra être évolutive pour répondre aux besoins de la GRC, qui est censée équiper d'un SGPN et de caméras corporelles entre 10 000 et 15 000 policiers et mettre le SGPN à la disposition d'autres utilisateurs dans l'organisation.

5.3 L'entrepreneur devra tenir compte des défis uniques de la GRC, comme la saisie et le stockage de preuves numériques dans des zones où la bande passante d'information est limitée; la capacité de la caméra à fonctionner dans une large plage de températures compte tenu de la diversité des territoires de compétence; ou l'activation et la saisie automatiques de preuves numériques dans des situations d'urgence et de stress élevé.

5.4 Dans le cadre d'un processus concurrentiel visant à qualifier les répondants, le Canada choisira un entrepreneur qui fournira, en tant que service, les éléments suivants :

5.4.1 **Caméras corporelles**

L'entrepreneur doit fournir 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 et réparation;
- élimination sécuritaire;
- renouvellement continu.

Voici quelques exemples d'équipement connexe :

- plusieurs options de fixation sur les uniformes;
- supports de fixation ou attaches;
- stations d'accueil et câbles de recharge connexes;
- mécanismes de déclenchement par Bluetooth (étui, arme à impulsions, voiture);
- serveurs physiques.

5.4.2 **SGPN**

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

- configuration 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 provenant de diverses sources;
- recherche et récupération de preuves numériques;
- capacité 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.

6. Capacités fonctionnelles, résultats et valeur opérationnelle

Le tableau suivant présente les outils et les capacités opérationnelles que le Canada prévoit mettre en œuvre dans le cadre de cette initiative. La liste des capacités servira à établir la portée fonctionnelle du projet et les exigences détaillées qui seront expliquées dans les étapes ultérieures du processus d'acquisition. Cette liste des capacités peut aussi évoluer durant le processus d'acquisition.

Secteur fonctionnel	Capacité	Valeur opérationnelle
Caméras corporelles	• **Robuste et facile à utiliser**	• Des caméras pouvant résister à l'usure subie durant le quart de travail d'un policier sans compromettre la sécurité de son utilisateur. • Des caméras qui s'activent facilement d'une seule main, tout en empêchant la désactivation accidentelle.
	• **Options flexibles et sécurisées de fixation sur les uniformes**	• Des caméras qui peuvent être installées dans l'espace disponible et qui s'harmonisent visuellement avec les uniformes de la GRC. • Des caméras compatibles avec plusieurs options de fixation sur les uniformes pour répondre à différents besoins opérationnels. • Des supports de caméra pouvant être fixés solidement à l'uniforme du policier.
	• **Fonctionnement dans les régions éloignées et rurales**	• Des caméras qui peuvent résister aux hivers et aux étés canadiens sans que son rendement soit affecté ou que sa capacité à enregistrer les événements pendant le quart de travail d'un policier soit compromise.

	• **Téléchargement automatisé des preuves numériques**	• Des processus de téléchargement qui peuvent être réalisés dans des zones géographiques urbaines, rurales et éloignées et qui n'entraînent pas de travail supplémentaire pour les policiers à la fin de leur quart. • 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**	• Une autonomie et une capacité de stockage suffisantes pour que le policier puisse capter sur vidéo tous les éléments requis pendant la durée de son quart de travail.
	• **Gestion de l'équipement**	• L'offre, la distribution, l'entretien, la réparation, le remplacement, la mise à niveau et l'élimination sécuritaires des caméras corporelles et de l'équipement connexe.
SGPN	• **Stockage en nuage des preuves numériques**	• Permettre le téléchargement sécuritaire de preuves numériques contenues dans les caméras corporelles ainsi que d'autres fichiers multimédias vers une solution de stockage en nuage. • 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 7.1.
	• **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 facile des preuves à divers intervenants externes dans plusieurs territoires de compétence partout au pays.
	• **Communication d'information**	• Permettre la communication d'information à différents niveaux, y compris la communication d'information géographique. • 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. • Respecter les exigences de sécurité du gouvernement du Canada en matière de nuage Protégé B.
	• **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 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**	• Fournir du soutien technique en tout temps et dans les deux langues officielles du Canada relativement à l'utilisation des caméras corporelles et du SGPN tout en respectant un ensemble de normes de service.
	• **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.

7. Exigences obligatoires prévues

On s'attend à ce que toute future offre d'appels comprenne les exigences OBLIGATOIRES suivantes. Celles-ci sont liées à la capacité de l'entrepreneur à développer et à mettre en œuvre une solution de caméras corporelles et de SGPN. La liste complète des exigences qui doivent être remplies pour la solution de caméras corporelles et de SGPN est en cours d'élaboration et sera fournie plus tard dans le processus d'approvisionnement.

7.1 Accessibilité

La solution de système 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.

La solution de système 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

7.2 Obligations en matière de sécurité

Les éléments suivants sont un sous-ensemble de la série plus vaste d'exigences relatives à la sécurité en cours d'élaboration et ne constituent pas une liste exhaustive.

7.2.1 Assurance d'une tierce partie : Certifications et rapports

L'entrepreneur doit s'assurer que les données organisationnelles, l'infrastructure de l'entrepreneur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements des services sont protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans les pratiques et les politiques de l'entrepreneur en matière de sécurité.

L'entrepreneur doit démontrer que les mesures 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 chaque couche de service (p. ex. IaaS, PaaS, SaaS) dans l'offre de services infonuagiques, y compris :

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.

7.2.2 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.

Dans le cas où l'entrepreneur a été évalué et validé au moyen 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 sécurité cybernétique (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. À cette fin, il doit fournir les documents suivants à la GRC :

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.

7.2.3 Supports amovibles/portables

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

7.2.4 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 sauvegardées ou conservées aux 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

a) un centre de données qui répond à toutes les exigences et certifications de sécurité indiquées à la section 38 en ce qui concerne la sécurité physique (centre de données/installations);
b) qui garantit l'impossibilité de trouver les données d'un client précis sur un support physique; et
c) qui utilise le chiffrement pour s'assurer qu'aucune donnée n'est gravée sur disque sous une forme non chiffrée, conformément à la section 19 - Protection cryptographique.

L'entrepreneur doit mettre en œuvre la capacité pour la GRC d'isoler les données organisationnelles hébergées dans les services infonuagiques 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 infonuagiques 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.

L'entrepreneur des services infonuagiques proposés a l'obligation permanente de notifier la GRC et/ou le Canada lorsque des mises à jour sont apportées à la liste des lieux physiques où peuvent se trouver les données organisationnelles.

7.2.5 Sauvegardes et reprises

Les sauvegardes doivent être stockées dans des centres de données séparés géographiquement d'au moins 200 km afin de les protéger contre les catastrophes naturelles ou d'origine humaine, et fonctionnant sur des réseaux électriques différents afin de garantir une protection contre les pannes de courant prolongées dans une région géographique donnée.

7.2.6 Gestion des incidents

Le processus d'intervention de l'entrepreneur en cas d'incident de sécurité pour les services infonuagiques doit englober le cycle de vie de la gestion des incidents de sécurité de la TI et les

pratiques de soutien 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://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; le 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 des procédures en place pour répondre aux demandes relatives à des éléments de preuve numériques potentiels ou à d'autres renseignements provenant de l'environnement des services infonuagiques, 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.

7.2.7 Protection cryptographique

Au minimum, la cryptographie validée selon la FIPS 140-2, niveau 1, est utilisée lorsque le chiffrement est nécessaire pour le système de gestion de preuves numériques.

7.2.8 Interfaces de programmation d'applications (API) externes

Des mesures raisonnables doivent être prises pour protéger les API externes au moyen de 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).

7.2.9 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 aux services infonuagiques, 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.

7.2.10 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 et/ou OpenID Connect 1,0 (ou versions ultérieures), où les justificatifs d'identité de l'utilisateur final et l'authentification aux services infonuagiques relèvent exclusivement 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.

7.2.11 **Emplacement des employés - Gestion des services à distance**

L'entrepreneur doit gérer et surveiller l'administration à distance du service infonuagique 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 infonuagiques 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 infonuagiques.

7.2.12 **Accès et vérification**

L'entrepreneur doit permettre au Canada d'examiner et d'analyser de façon centralisée les dossiers de vérification provenant des composants du service d'abonnement, ce qui comprend, 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 protocole d'application pour le service d'abonnement 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.

7.2.13 **Fuite d'information**

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 en cause dans la contamination d'un système;
c) un processus visant à isoler et à éradiquer un système contaminé; et
d) un processus permettant de déterminer les systèmes qui pourraient avoir été contaminés par la suite et toute autre mesure prise pour empêcher une nouvelle contamination.

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

7.2.14 **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.

7.2.15 **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.

7.2.16 **Gestion des risques liés à la chaîne d'approvisionnement**

Dans le cas où l'entrepreneur est un fournisseur SaaS (logiciel comme service) utilisant un fournisseur IaaS (infrastructure comme service) ou PaaS (plateforme comme service) approuvé par le gouvernement du Canada qui se conforme déjà aux exigences de la section 38 - Gestion des risques liés à la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur SaaS utilisant le fournisseur IaaS approuvé par le gouvernement du Canada doit fournir une liste de produits de la technologie de l'information et des communications (TIC) qui décrit le matériel TIC déployé dans l'environnement du fournisseur IaaS approuvé par le gouvernement du Canada aux fins d'examen de l'intégrité de la chaîne d'approvisionnement (ICA).

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

Traitement des préoccupations relatives à la sécurité

Nonobstant le point précédent, si le 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 les services et/ou les produits indiqués 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.

7.2.18 **Programme de sécurité industrielle – Exigences relatives à la sécurité pour les fournisseurs canadiens**

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/.

7.3 **Tâches**

7.3.1 **Aperçu**

L'entrepreneur aura pour responsabilité principale d'accomplir les tâches suivantes en ce qui concerne le lancement, le déploiement et l'opérationnalisation des caméras corporelles et du SGPN :

- Planification de l'intégration
- Planification et mise en œuvre
- Soutien à la formation et à la gestion du changement organisationnel
- Déploiement
- Phase d'exploitation
- Innovation et amélioration des services
- Autres services

Les rubriques ci-dessous présentent un aperçu des diverses tâches attendues de l'entrepreneur.

D'autres descriptions, la portée du projet, les rôles, les responsabilités, l'information sur le statut actuel et les exigences seront examinés et précisés de concert avec les fournisseurs qualifiés de l'IQ (invitation à se qualifier) à l'étape de la demande de propositions.

7.3.2 **Planification de l'intégration**

On s'attend à ce que l'entrepreneur assure des services professionnels au gouvernement du Canada pour déterminer la meilleure façon de déployer les caméras corporelles et le SGPN à l'échelle du pays. Pour ce faire, il doit notamment se pencher sur les principaux éléments à prendre en considération en vue du déploiement afin d'optimiser les chances de réussite et d'assurer une gestion des risques, en se fondant sur l'expérience acquise dans la gestion des déploiements ayant une portée et une envergure comparables à ceux exigés. La planification comprend également un soutien l'établissement du nombre de ressources canadiennes nécessaires à la réussite du processus d'intégration ainsi que du nombre de ressources requises sur une base permanente pour la gestion de l'équipement, le caviardage et la modification des renseignements numériques, et la divulgation des données. Les livrables connexes seront définis plus précisément dans les demandes de soumissions qui en résulteront, s'il y a lieu.

7.3.3 **Planification et mise en œuvre**

On s'attend à ce que l'entrepreneur assure des services de mise en œuvre, y compris la gestion et la planification de projets, la conception de systèmes, de données et de processus, la mise en œuvre de solutions, la configuration, l'établissement de liens avec les systèmes canadiens, 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 informatique 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.).

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

On s'attend à ce que l'entrepreneur offre une expertise et les ressources nécessaires pour soutenir l'élaboration d'un plan de formation et de gestion du changement reposant sur l'expérience acquise avec d'autres solutions d'une ampleur comparable. On y présente un aperçu des principales étapes que chaque division et détachement doit entreprendre pour se préparer à l'intégration ainsi que des listes de vérification ou une évaluation de l'état de préparation à remplir avant l'intégration. De plus, l'entrepreneur doit contribuer aux politiques et aux procédures provisoires 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. On s'attend également à ce que l'entrepreneur apporte des outils et du matériel de formation qui pourront être intégrés aux programmes de formation générale à l'intention des policiers.

7.3.5 **Déploiement**

7.3.5.1 **Déploiement initial**

Il est attendu que l'entrepreneur prendra en charge un déploiement initial de caméras corporelles dans un secteur rural, une région éloignée et un centre urbain. Il s'agira alors de faire l'essai d'un certain nombre d'éléments, notamment les caméras, le 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.

7.3.5.2 **Ajustements reposant sur le déploiement initial**

Il est attendu que le gouvernement du Canada réalisera une évaluation officielle du déploiement initial et que l'entrepreneur prendra en charge les mises à jour et les modifications nécessaires aux caméras corporelles et au SGPN, aux procédures et aux outils et au matériel de formation.

7.3.5.3 **Déploiement progressif**

Il est attendu que l'entrepreneur prendra en charge un déploiement progressif des caméras corporelles et du SGPN à l'échelle du pays. L'entrepreneur devra soutenir la planification du déploiement progressif et fournir des conseils et une orientation relativement à la séquence et à l'ampleur de chaque phase du déploiement en fonction des leçons tirées du déploiement initial.

7.3.5.4 **Phase d'exploitation**

L'entrepreneur devra assurer la gestion et le soutien des services des caméras corporelles et du SGPN après chaque phase du déploiement conformément à une entente contractuelle prévoyant un ensemble de responsabilités et de normes de service.

7.3.5.5 **Innovation et amélioration des services**

On s'attend à ce que l'entrepreneur assure des services au gouvernement du Canada et qu'il travaille en collaboration avec celui-ci afin d'innover et d'apporter des améliorations à ses services. Il s'agira notamment de proposer de nouvelles technologies et de nouveaux processus afin d'améliorer l'utilisation par le gouvernement du Canada des caméras corporelles et du SGPN et d'en optimiser la capacité.

7.3.5.6 **Autres services**

On pourrait demander à l'entrepreneur d'assurer d'autres services au 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).