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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving Public Works and Government Services Canada/Réception des soumissions Travaux publics et Services gouvernementaux Canada
800 Burrard Street, Room 219
800, rue Burrard, pièce 219
Vancouver, BC V6Z 0B9
Bid Fax: (604) 775-7526

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Solution infonuagique de collecte e

Solicitation No. - N° de l'invitation M2989-190834/A	**Date** 2018-06-26
Client Reference No. - N° de référence du client M2989-190834	**GETS Ref. No. - N° de réf. de SEAG** PW-$VAN-590-8377
File No. - N° de dossier VAN-8-41052 (590)	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2018-07-19

Time Zone
Fuseau horaire
Pacific Daylight Saving Time PDT

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

Address Enquiries to: - Adresser toutes questions à: Sezginalp, Kipp	**Buyer Id - Id de l'acheteur** van590
Telephone No. - N° de téléphone (604) 367-5341 ( )	**FAX No. - N° de FAX** (604) 775-7526

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

RCMP, Info Mgmt & Tech Branch
MAILSTOP #1505, RCMP EHQ
14200 GREEN TIMBERS WAY
SURREY
British Columbia
V3T 6P3
Canada

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	**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
Public Works and Government Services Canada - Pacific Region
219 - 800 Burrard Street
800, rue Burrard, pièce 219
Vancouver, BC V6Z 0B9

Canada

CECI N'EST PAS UNE DEMANDE DE SOUMISSIONS

Il S'AGIT D'UNE DEMANDE DE RENSEIGNEMENTS (DR) AUPRÈS DE L'INDUSTRIE

La présente DR de Services publics et Approvisionnement Canada (SPAC) vise à recueillir des commentaires pour la Gendarmerie royale du Canada (GRC) sur tous les aspects précisés dans la présente. Les commentaires recueillis permettront à la GRC de connaître l'opinion des entreprises de l'industrie et de fournir à ces dernières une période raisonnable leur permettant de se préparer en vue d'une éventuelle demande de propositions (DP) subséquente.

Remarque à l'intention des répondants éventuels

Une réponse à la présente DR n'est pas une condition préalable à remplir pour recevoir, le cas échéant, la demande de soumissions qui pourrait découler du présent processus. Ce processus de consultation n'est pas une invitation à soumissionner et ne sera pas utilisé aux fins d'une présélection ou pour restreindre autrement la participation à une future demande de soumissions. Aucune liste restreinte de fournisseurs en vue de la réalisation de travaux ultérieurs ne sera établie à la suite de la présente DR. Les répondants éventuels sont priés de faire part de leur intérêt en répondant aux questions du présent processus de consultation.

La publication de la présente DR n'oblige pas la GRC à lancer un appel d'offres subséquent et ne l'engage pas, juridiquement ou de toute autre façon, à conclure une entente ou à accepter les suggestions présentées par l'industrie. La GRC se réserve le droit d'accepter ou de rejeter une partie ou l'ensemble des commentaires reçus.

Les répondants éventuels sont avisés que toute information transmise à la GRC en réponse au processus de consultation de l'industrie pourra être utilisée par cette dernière aux fins de l'élaboration d'une demande de soumissions concurrentielle subséquente. Toutefois, la GRC n'est pas tenue de donner suite à quelque déclaration d'intérêt, ni d'en tenir compte dans un document connexe, par exemple, une demande de soumissions. La présente DR ne doit nullement être considérée comme une autorisation donnée par la GRC aux répondants d'entreprendre tout travail qui entraînerait des frais pour la GRC. La GRC ne sera pas tenue responsable des coûts, des honoraires ou des frais engagés pour préparer ou présenter une réponse à la DR et ne les remboursera pas. La GRC ne sera liée d'aucune façon par le contenu du présent document. Elle se réserve le droit de modifier, en tout temps, une partie ou la totalité des exigences, si elle le juge nécessaire.

1. TRANSMISSION DES RÉPONSES

Les réponses peuvent être transmises par courrier électronique (format MS Word), par télécopieur ou sur papier directement au responsable de la DR indiqué sur la page couverture de la présente DR.

2. RÉPONSES DE L'INDUSTRIE

Présentation des réponses

Il n'y a pas de limite imposée quant au nombre de pages de renseignements fournis. Les répondants doivent répondre à toutes les questions posées à l'annexe A. Veuillez répondre en indiquant le numéro des questions correspondantes posées à l'annexe A.

Le nom et l'adresse de retour du répondant, le numéro de DR et la date de clôture doivent apparaître clairement sur la réponse. Les réponses à la présente DR ne seront pas retournées.

Confidentialité

Les répondants sont priés d'indiquer clairement les éléments de réponse qui sont de nature exclusive ou confidentielle. La réponse de chaque répondant demeurera confidentielle.

3. DEMANDES DE RENSEIGNEMENTS

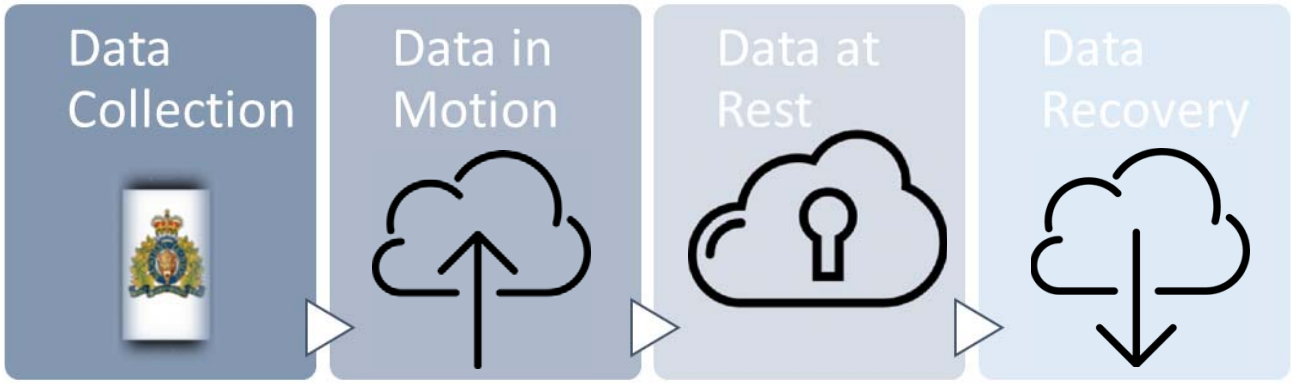
Toutes les demandes de renseignements et autres questions à l'égard de la présente DR doivent être envoyées au responsable de la DR mentionné précédemment. Le Canada pourra réviser les questions, ou demander au répondant de le faire, afin d'en éliminer le caractère exclusif et de permettre que les réponses soient communiquées à toutes les parties intéressées.

ANNEXE A

Énoncé de travail

Demande de renseignements :
Solution infonuagique de collecte et de gestion des preuves numériques

Projet : Système électronique de gestion des preuves numériques



1. Introduction

1.1. À l'heure actuelle, la GRC recueille des preuves dans un large éventail de formats numériques comme des photos, des vidéos et des enregistrements audio, et leur nombre augmente rapidement. Elle stocke ces preuves à l'aide de plusieurs solutions matérielles, logicielles et procédurales. La gestion uniforme et efficace des preuves représente une tâche difficile, et le niveau de soutien nécessaire au stockage sur le matériel informatique et en raison des limites associées au cycle de vie est considérable.

1.2. Conformément à la Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada, la GRC a besoin d'une solution logicielle pour recueillir, stocker, organiser, protéger, communiquer et éliminer des preuves numériques sous la forme d'un logiciel en tant que service (SaaS).

1.3. Les renseignements fournis par les répondants à la présente DR peuvent être utilisés pour redéfinir les exigences, la stratégie d'approvisionnement ou l'enveloppe budgétaire actuelles du projet. Les renseignements recueillis au moyen de la DR peuvent également être utilisés pour aider le Canada dans le cadre de l'élaboration d'un essai de validation de principe ou d'une demande de propositions (DP) concurrentielle.

2. Garantie, service à la clientèle et modèle de coûts

2.1. La présente DR vise à déterminer la disponibilité et la maturité d'une solution SaaS qui répond aux besoins actuels de la GRC et qui continuera à évoluer en fonction des pratiques actuelles et des besoins opérationnels des services de police au Canada.

2.1.1. Veuillez décrire la taille et la portée des organismes (leur nombre) qui utilisent votre application de collecte de preuves et solution de gestion des preuves numériques (SGPN) SaaS au Canada et dans le monde, et indiquer depuis combien d'années ils l'utilisent. Veuillez préciser depuis combien de temps votre entreprise œuvre dans cette industrie.

2.1.2. Décrivez les options de formation pour les utilisateurs et les administrateurs, ainsi que toutes les options de spécialisation à l'intérieur du Canada.

2.1.3. Décrivez les options de garantie et de maintenance pour toutes les composantes de la solution.

2.1.4. Y a-t-il un service de soutien à la clientèle offert 24 heures sur 24, 7 jours sur 7? Décrivez l'ensemble des options de soutien, des niveaux de service et des outils disponibles, y compris le soutien bilingue (anglais et français) offert.

2.2. La GRC devra comprendre le modèle de coûts associé à l'utilisation de l'application de collecte et à l'utilisation et au stockage de l'application SaaS, ainsi que les autres coûts connexes ou supplémentaires. Veuillez décrire tous les modèles de coûts associés à l'utilisation de cette solution et tous les facteurs de coût particuliers demandés ci-dessous :

2.2.1. Décrivez les coûts de la réalisation d'un essai de validation de principe de six mois, à compter de l'été 2018, aux détachements de la GRC du Lower Mainland de la C.-B., auprès d'un nombre maximal de 200 utilisateurs.

2.3. Décrivez les outils disponibles pour effectuer un suivi de l'utilisation et de la performance du système et toutes les options de rapport sur les indicateurs de performance clés (IPC) offertes aux clients.

2.4. Décrivez en quoi la solution est conforme à la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) et à toute autre norme de gestion de l'information de la police canadienne, notamment les statistiques obtenues par le biais de la Déclaration uniforme de la criminalité (DUC).

3. Collecte de données

3.1. La GRC recueille actuellement des preuves numériques sur le terrain à l'aide de nombreux appareils différents comme des appareils photographiques, des caméras, des enregistreurs et des ordinateurs, et cherche à se prévaloir d'une application normalisée qui permet de recueillir facilement plusieurs formats de preuves numériques d'une manière sécurisée et efficace.

3.2. La GRC souhaite que l'application de collecte mobile prenne en charge un certain nombre de plateformes matérielles différentes, notamment les appareils Windows et les téléphones intelligents Android :

3.2.1. Indiquez les plateformes d'appareils prises en charge par votre application de collecte de preuves et toutes les dépendances, conditions ou spécifications connexes nécessaires.

3.3. Décrivez de quelle façon l'identification et l'authentification sont sécurisées dans l'application, notamment toutes les capacités ou exigences d'authentification à deux facteurs (A2F), notamment l'intégration d'Active Directory (AD) ou de la gestion des appareils mobiles (GAM).

3.4. La GRC a besoin de recueillir des photos, des vidéos et des enregistrements audio à l'aide de l'application de collecte mobile :

3.4.1. Décrivez de quelle façon l'appareil permet de garantir la sécurité des preuves et d'établir leur authenticité avant de les transmettre à la solution infonuagique SaaS.

3.4.2. Indiquez les métadonnées qui sont recueillies automatiquement ou manuellement par l'utilisateur ou le logiciel de l'application de collecte.

3.4.3. Décrivez de quelle façon ces données sont éliminées de l'appareil suivant leur transfert dans la solution infonuagique SaaS.

3.5. La GRC souhaite recueillir des preuves de tierces parties à l'aide de l'application de collecte :

3.5.1. Décrivez de quelle façon la solution permet aux membres du public de soumettre des preuves sur photos, vidéos ou enregistrements audio de façon sécurisée dans le système par le biais d'Internet, ainsi que toutes les répercussions connexes sur la sécurité (y compris la détection des virus), les examens et les coûts.

3.6. La solution permet-elle la présentation en masse de preuves par le public? Veuillez décrire le fonctionnement de cette fonction et toutes les répercussions connexes sur la sécurité, les examens, le stockage et les coûts.

3.7. Dans l'application de collecte, décrivez les autres formats de fichier qu'un client mobile, un client Web ou un client lourd peut importer, stocker et gérer ou manipuler à l'aide de la solution, ainsi que les limites relatives à la taille de ces fichiers.

4. Données en mouvement

4.1. Étant donné que la GRC recueille actuellement des preuves numériques sur le terrain à l'aide de nombreux appareils différents comme des appareils photographiques, des caméras, des enregistreurs et des ordinateurs, le transport de ces renseignements vers les espaces de stockage dorsal et les processus dorsaux n'est pas toujours uniforme et nécessite une attention toute particulière et un traitement manuel. La GRC cherche une solution qui permet la transmission sécuritaire de ces preuves dans une solution de stockage.

4.2. Pour ce qui est de la connexion de l'application de collecte mobile à la solution infonuagique SaaS, la GRC a besoin d'assurer la sécurité de la transmission par Internet des renseignements « Protégé B » conformément à l'AMPTI 2017-02 du gouvernement du Canada qui stipule que *toutes les données électroniques du GC de catégorie « Protégé B », « Protégé C » et « classifiées » en transit doivent être chiffrées lorsqu'elles sont en transit à l'extérieur des zones des opérations et de sécurité contrôlées par le GC au Canada ou à l'étranger* :

4.2.1. Décrivez en quoi votre solution répond aux exigences de l'AMPTI 2017-02 ou les dépasse.

4.2.2. Décrivez en quoi votre solution répond aux exigences de l'ITSP 40.111 *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* du Centre de la sécurité des télécommunications (CST) ou les dépasse.

4.2.3. Décrivez toutes les composantes de sécurité de réseau que la GRC devrait fournir.

4.3. Décrivez toutes les considérations particulières relatives à la largeur de bande, à la transmission ou à l'extensibilité (pour un accès et un stockage simultanés) pour l'application de collecte de preuves, l'accès à l'application SaaS et tout autre logiciel client fourni ou requis.

4.4. Décrivez tous les coûts liés au téléversement et au téléchargement de données dans le cadre de la solution, excluant les coûts liés à la largeur de bande des appareils sans fil.

5. Données au repos

5.1. La GRC stocke actuellement les preuves numériques dans un certain nombre de systèmes différents et utilise de nombreux processus différents, y compris le stockage sur DVD. À des fins d'uniformité, de sécurité et d'efficacité, elle souhaite que ces preuves numériques soient stockées et gérées de façon centralisée par la solution.

5.2. La GRC a besoin que le stockage, la sauvegarde et le traitement des données s'effectuent en totalité au Canada conformément à l'AMPTI 2017-02 du gouvernement du Canada qui stipule que *toutes les données électroniques des catégories «Protégé B », « Protégé C » et « classifiées » doivent avoir un contrôle positif continu dans une installation informatique approuvée par le GC située dans les frontières géographiques du Canada ou dans les locaux d'un ministère du GC situé à l'étranger, comme une mission diplomatique ou consulaire* :

5.2.1. Décrivez en quoi votre solution répond aux exigences de l'AMPTI 2017-02 relatives à la résidence des données ou les dépasse.

5.2.2. Décrivez de quelle façon les données au repos peuvent être chiffrées et indiquez si ou comment cette méthode permet de renforcer les clés des agences.

5.2.3. Décrivez en quoi votre solution est conforme au Profil de contrôle de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage.

5.2.4. Décrivez en quoi votre solution est conforme à l'Avis de mise en œuvre de la Politique sur la sécurité du gouvernement du Canada AMOPS 2017-01 *Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage.*

5.2.5. Indiquez l'emplacement du serveur, l'emplacement de sauvegarde et tout autre emplacement de stockage de votre solution infonuagique SaaS :

5.2.5.1. Ces services sont-ils géoredondants au Canada?

5.2.5.2. Veuillez indiquer le fournisseur de services infonuagiques utilisé, l'emplacement des centres de données, y compris les fournisseurs sous-jacents de plateformes (PaaS) ou d'infrastructures (IaaS), le niveau de service offert et les mesures de sauvegarde des données.

5.2.5.3. Décrivez de quelle façon le système empêche l'accès de l'extérieur du Canada ou l'élimination des données à partir du Canada.

5.2.5.4. Décrivez de quelle façon l'accès de soutien du fournisseur aux données est géré et minimisé. La GRC exigera que tout membre du personnel du fournisseur et tout fournisseur de services infonuagiques qui peut avoir accès aux données obtiennent une attestation de sécurité de la GRC.

5.3. En ce qui concerne votre solution de gestion des preuves, veuillez décrire les stratégies d'évaluation de la sécurité appliquées et toutes les certifications en place, notamment les

normes ISO/IEC 27001, 27017 et 27018, et toute autre norme pertinente, et :

5.3.1. Décrivez les processus de surveillance et d'assurance connexes en place et la façon dont ils sont gérés.

5.3.2. La solution infonuagique et l'application SaaS font-elles l'objet d'une surveillance 24 heures sur 24, 7jours sur 7, à des fins de gestion des événements, de sécurité et de mesure de la performance des applications?

5.3.3. Indiquez de quelle façon ces normes sont évaluées et vérifiées, à quel intervalle et par qui.

5.4. Décrivez les options qu'offre le système pour les alertes relatives aux fichiers, les dates d'agenda et toute autre fonction de supervision :

5.4.1. Décrivez les options de personnalisation du flux de travail offertes et la façon de les configurer pour plusieurs lieux ou territoires de compétence?

5.4.2. Décrivez la capacité du système afin de restreindre l'accès aux fichiers, de réattribuer des fichiers et de fournir un modèle d'accès sécurisé fondé sur les rôles.

5.5. Décrivez de quelle façon la solution communique les preuves aux utilisateurs internes et aux partenaires externes comme la Couronne, et :

5.5.1. Décrivez de quelle façon la sécurité est gérée lors des échanges avec des partenaires externes et comment ces aspects sont intégrés dans les processus des pistes de vérification et d'authentification.

5.6. Décrivez les considérations et les coûts liés à l'espace de stockage, à la conservation et à l'extensibilité. La solution peut-elle être adaptée rapidement pour répondre aux besoins opérationnels?

5.7. Décrivez de quelle façon l'identification et l'authentification sont sécurisées dans la solution, notamment toutes les capacités d'authentification à deux facteurs (A2F) qui renforcent les certificats des organismes, notamment l'intégration d'Active Directory (AD) et de l'authentification unique (SSO).

5.8. Décrivez les options de piste de vérification offertes afin d'effectuer un suivi des utilisateurs internes, des partenaires externes et des administrateurs des services dorsaux qui ont consulté, exporté ou manipulé des preuves ou des documents.

5.9. Décrivez de quelle façon la solution gère la conservation des preuves et des fichiers. Les périodes de conservation peuvent-elles être personnalisées et liées aux codes de déclaration des organismes dans le cadre de la DUC ou sont-elles établies dans le Système de gestion des documents (SGD) d'un organisme?

5.9.1. Décrivez de quelle façon les périodes de conservation peuvent être mises en suspens temporairement en vue de respecter les moratoires sur la destruction.

5.10. Décrivez de quelle façon la solution permettra la mise sous séquestre des fichiers et des preuves afin de satisfaire aux exigences de la *Loi sur le système de justice pénale pour les adolescents*, de la *Loi sur le casier judiciaire* et de toute autre exigence relative à l'absolution inconditionnelle.

5.10.1. Décrivez de quelle façon les contrôles d'accès fondés sur les rôles peuvent être personnalisés pour s'adapter aux changements dans la confidentialité des fichiers.

6. Récupération de données

6.1. À la fin d'un essai de validation de principe, d'un projet pilote ou d'un contrat, il se peut que la GRC ait besoin de récupérer certaines des données ou la totalité d'entre elles :

6.1.1. Décrivez les solutions offertes pour récupérer des données à partir du nuage sur le site SaaS du fournisseur et les transférer sur un site de plateforme en tant que service (PaaS) contrôlé par la GRC.

6.1.2. Décrivez les solutions et les options de format qui sont offertes pour récupérer des données à partir du nuage SaaS et les transférer dans une solution de stockage sur place à la GRC.

7. Autres services connexes

7.1. Décrivez tout autre outil à valeur ajoutée que peut fournir votre solution SaaS et indiquez si ces solutions sont offertes dans le cadre de la solution de base, d'une option moyennant un coût ou d'un développement futur prévu (et notez l'année ou le trimestre prévu). Ces outils à valeur ajoutée peuvent comprendre notamment ce qui suit :

7.1.1. Décrivez les outils de rédaction offerts pour la rédaction de vidéos ou d'enregistrements audio. Ces outils sont-ils automatisés ou peuvent-ils l'être?

7.1.1.1. Ces outils permettent-ils de conserver le fichier original et les métadonnées?

7.1.1.2. Ces outils sont-ils inclus dans les journaux de saisie des pistes de vérification?

7.1.2. Décrivez tous les outils de transcription automatisés offerts pour la transcription du texte des enregistrements audio ou vidéo.

7.1.3. Décrivez toutes les capacités de l'interface de programme d'application (IPA) du système, y compris les capacités existantes de l'interface du Système de gestion des documents (SGD) et du Système de gestion des cas graves (GCG).

7.1.4. Décrivez toutes les capacités relatives aux normes sur les données en matière d'application de la loi (LEIDS) de l'Association canadienne des chefs de police (ACCP) en fonction du

Modèle national d’échange de l’information (NIEM).

7.1.5. Indiquez si vous utilisez ou prévoyez utiliser un mécanisme de sécurité fondé sur des chaînes de blocs dans le cadre de la solution.

7.2. Indiquez toutes les installations de gestion de la sécurité qui assurent une gestion de la sécurité du réseau, des ressources informatiques, du stockage, des données et des applications, et les protègent contre les menaces de façon uniforme.

7.3. Décrivez toutes les options et les solutions d’intégration offertes à l’appui des systèmes de caméras vidéo corporelles (CVC).

7.4. Décrivez toutes les options et les solutions d’intégration offertes à l’appui des systèmes vidéo automobiles (SVA).

7.5. Décrivez toutes les options et les solutions d’intégration offertes à l’appui des solutions d’enregistrement des salles d’entrevue.

7.6. Décrivez toutes les options et les solutions d’intégration offertes à l’appui des solutions de caméras de sécurité de télévision en circuit fermé (TVCF).

7.7. Décrivez toutes les options et les solutions d’intégration offertes à l’appui des journaux des événements liés aux armes à impulsions et de la surveillance de la santé.

7.8. Décrivez toutes les options et les solutions d’intégration offertes pour la divulgation électronique à la Couronne.

7.9. Décrivez toutes les options et les solutions d’intégration offertes pour l’analyse des renseignements organisationnels.

7.10. Décrivez toute autre option ou solution d’intégration offerte.