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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Application Software-RFI

Solicitation No. - N° de l'invitation	Date
G9292-211695/A	2019-02-14
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
G9292-211695	PW-$$XL-108-34622
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
108xl.G9292-211695	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-03-06

Time Zone
Fuseau horaire
Eastern Standard Time
EST

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Fenwick, Wesley	108xl
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 720-7743 ( )	( ) -

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

EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA
NCR - Gatineau
140 PROMENADE DU PORTAGE
GATINEAU
Quebec
K1A0J9
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	Delivery Offered - Livraison proposée
See Herein	

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

Canada

ANNEXE A – ÉBAUCHE DE LA DEMANDE DE RENSEIGNEMENTS (DDR)

Solution logicielle pour la surveillance des activités des employés et de l'accès à l'information sur les applications d'entreprise

(SAEAIE)

TABLE DES MATIÈRES

DEMANDE DE RENSEIGNEMENTS CONCERNANT

DES APPLICATIONS D'ENTREPRISE POUR LA SURVEILLANCE DES ACTIVITÉS DES EMPLOYÉS ET DE L'ACCÈS À L'INFORMATION (SAEAIE)

POUR

EMPLOI ET DÉVELOPPEMENT SOCIAL CANADA

PARTIE A

1. C`ontexte et objet de la présente demande de renseignements (DDR)

a) Emploi et Développement social Canada (EDSC) publie la présente demande de renseignements (DDR) pour solliciter auprès de fournisseurs des renseignements sur les solutions disponibles sur le marché pour « surveiller les activités des employés et l'accès à l'information à l'aide d'applications d'entreprise » (ci-après appelée « solution ») qui contiennent des renseignements de nature délicate.

2. Nature de la demande de renseignements

a) Il ne s'agit pas d'un appel d'offres. Par conséquent, les fournisseurs éventuels des biens ou des services décrits dans la présente DDR ne devraient pas réserver des stocks ou des installations, ni affecter des ressources, en fonction des renseignements qui y sont présentés. La présente DDR ne donnera pas lieu à la création de listes de fournisseurs. Par conséquent, le fait qu'un fournisseur éventuel réponde ou non à la présente DDR ne l'empêchera pas de participer à tout processus d'approvisionnement ultérieur. En outre, la présente DDR n'entraînera pas nécessairement l'achat de l'un ou de l'autre des biens et des services qui y sont décrits. La présente DDR sert simplement à solliciter des renseignements et des commentaires de l'industrie sur les questions qui y sont abordées.

3. Nature et format des réponses

a) Les répondants sont priés de formuler leurs commentaires, leurs préoccupations et, le cas échéant, d'autres recommandations concernant la façon dont pourraient être satisfaits les exigences ou les objectifs décrits dans la présente DDR. Ils sont également invités à commenter le contenu, la présentation et l'organisation des documents préliminaires joints à la présente DDR. Les répondants sont priés d'expliciter les hypothèses qu'ils avancent dans leur réponse.

4. Coûts associés aux réponses

a) Le Canada ne remboursera pas aux répondants les dépenses engagées pour répondre à la présente DDR.

5. Traitement des réponses

a) **Utilisation des réponses :** Les réponses ne feront pas l'objet d'une évaluation officielle. Toutefois, le Canada pourra utiliser ces réponses pour élaborer ou modifier ses stratégies d'acquisition ou tout document préliminaire joint à la présente DDR. Le Canada examinera

toutes les réponses reçues d'ici la date de clôture de la DDR. Cependant, s'il le juge opportun, il pourra examiner aussi les réponses reçues après la date de clôture de la DDR.

b) **Équipe d'examen :** Une équipe d'examen composée de représentants de Services publics et Approvisionnement Canada (SPAC) étudiera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou de faire appel à des ressources du gouvernement, s'il le juge nécessaire, pour l'examen des réponses. Les réponses ne seront pas nécessairement toutes examinées par l'ensemble des membres de l'équipe d'examen s.

c) **Confidentialité :** Les répondants devraient indiquer toutes les parties de leurs réponses qu'ils jugent exclusives ou confidentielles. EDSC traitera ces renseignements de façon confidentielle, conformément à la *Loi sur l'accès à l'information*.

d) **Rencontres postérieures à l'examen des présentations :** EDSC peut, à sa discrétion, demander des rencontres postérieures à l'examen des présentations avec des répondants sélectionnés afin de fournir des précisions sur l'information fournie ou les inviter à effectuer une présentation sur une partie ou la totalité de la solution proposée. Au besoin, ces rencontres auront lieu à l'endroit le plus approprié, qui sera déterminé à une date ultérieure. Le but de ces rencontres sera de permettre une discussion en personne avec les répondants. Bien que les répondants puissent demander une réunion et que leur demande sera prise en considération, le Canada déterminera s'il a besoin de renseignements supplémentaires de la part d'un répondant donné et organisera des rencontres en conséquence. Toutes les demandes des répondants doivent être transmises à l'autorité contractante. Notez qu'un maximum de deux heures sera réservé pour toute rencontre avec les répondants. Tous les coûts associés aux rencontres postérieures à l'examen des présentations, y compris les frais de déplacement, seront assumés par le répondant.

e) Les renseignements recueillis dans le cadre de la présente DDR serviront à orienter la DDP requise pour l'acquisition d'une solution de surveillance des activités des employés et de l'accès à l'information.

f) La présente DDR contient un aperçu et un résumé des programmes associés à l'acquisition d'une solution de surveillance des activités des employés et de l'accès à l'information. Les fournisseurs intéressés sont priés de communiquer avec l'autorité contractante pour obtenir des détails supplémentaires qui fourniront plus de contexte et indiqueront les questions précises adressées à l'industrie.

6. Données volumétriques

a) Les projections de volume de la Partie B sont fournies aux répondants uniquement à des fins d'information. Bien qu'elles représentent la meilleure information dont dispose actuellement SPAC, le Canada ne garantit pas que les données sont complètes ou exemptes d'erreurs.

7. Format des réponses

a) **Page couverture :** Si la réponse est donnée en plusieurs volumes, les répondants sont priés d'indiquer sur la page couverture de chaque volume le titre de la réponse, le numéro de la demande de renseignements, le numéro du volume et leur dénomination sociale complète.

b) **Page titre :** La première page de chaque volume de la réponse, qui suit la page couverture, devrait être la page titre et contenir :

le titre de la réponse du répondant et le numéro du volume;

le nom et l'adresse du répondant;

le nom, l'adresse et le numéro de téléphone de la personne-ressource désignée par le répondant;

la date;

le numéro de la DDR

c) **Système de numérotation :** Les répondants sont priés d'utiliser dans leur réponse le système de numérotation correspondant à celui de la présente DDR. Les renvois à des documents descriptifs, à des manuels techniques et à des brochures accompagnant la réponse doivent respecter ce même système.

d) **Nombre de copies :** Le Canada demande aux répondants de soumettre une copie électronique de leurs réponses par courriel à l'autorité contractante indiquée dans les présentes.

8. Demandes de renseignements

a) Comme il ne s'agit pas d'une invitation à soumissionner, le Canada ne répondra pas nécessairement par écrit à toutes les demandes de renseignements ni ne distribuera forcément les réponses à tous les fournisseurs éventuels. Toutefois, les répondants qui ont des questions relatives à la DDR peuvent s'adresser à la personne suivante :

Autorité contractante :	Wesley Fenwick
Courriel :	Wesley.Fenwick@tpsgc-pwgsc.gc.ca
Téléphone :	613-720-7743

9. Présentation des réponses

a) **Date et lieu de présentation des réponses :** Les fournisseurs intéressés devraient présenter leur réponse à l'autorité contractante dont le nom est indiqué ci-dessus, au plus tard à l'heure et à la date indiquées à la page 1 de la présente demande.

b) **Responsabilité quant au respect du délai de livraison : I**l incombe à chaque répondant de s'assurer que sa réponse soit livrée à la bonne adresse et qu'elle soit reçue dans les délais prescrits.

c) **Identification des réponses :** Chaque répondant devrait s'assurer que son nom et son adresse, le numéro de la demande de renseignements et la date de clôture figurent lisiblement dans sa réponse.

PARTIE B

1. Aperçu de l'organisation

a) Employés et Développement social Canada (EDSC) est un ministère du gouvernement du Canada responsable des programmes sociaux et du marché du travail au niveau fédéral. EDSC a pour mission de bâtir un Canada plus fort et plus inclusif, d'aider les Canadiens à mener une vie productive et enrichissante et d'améliorer leur qualité de vie.

b) EDSC offre un éventail de programmes et de services qui touchent les Canadiens tout au long de leur vie. Le Ministère offre aux aînés une sécurité de revenu de base, soutient les travailleurs sans emploi, aide les étudiants à financer leurs études postsecondaires et aide les parents qui élèvent de jeunes enfants. Le Programme du travail contribue au bien-être social et économique en favorisant des milieux de travail sécuritaires, sains, équitables et inclusifs, ainsi que des relations de travail coopératives dans les secteurs de compétence fédérale. Service Canada aide les citoyens à accéder aux programmes d'EDSC ainsi qu'à d'autres programmes et services du gouvernement du Canada.

c) En particulier, le Ministère est responsable de distribuer plus de 120 milliards de dollars en prestations directement aux particuliers et aux organisations par l'entremise de programmes et de services du gouvernement du Canada comme l'assurance-emploi, la Sécurité de la vieillesse, le Régime de pensions du Canada et le Programme canadien de prêts aux étudiants. Le Ministère fournit également 1,8 milliard de dollars en financement à d'autres ordres de gouvernement, à des éducateurs et à des organismes des secteurs bénévole et privé.

2. Description de l'environnement actuel

a) EDSC compte actuellement environ 24 000 employés et plus de 500 applications d'entreprise (dont une centaine sont essentielles à la mission) qui sont mis à contribution pour exécuter son mandat. Les employés et l'utilisation des applications sont dispersés partout au Canada, et l'administration centrale est située à Ottawa (Ontario). Bon nombre de ces applications sont utilisées pour fournir des prestations aux citoyens. Il s'agit de systèmes sur mesure et ils seront modernisés au cours de la prochaine décennie. La majorité de ces applications renferment des renseignements de nature délicate auxquels le personnel interne a accès pour s'acquitter de ses fonctions. Certains systèmes sont dotés de fichiers journaux qui fournissent de l'information sur l'activité de l'utilisateur sur l'application, mais la qualité et la convivialité des fichiers journaux varient d'une application à l'autre et certaines applications n'ont pas de fichiers journaux. Les applications d'entreprise sont accessibles au moyen d'ordinateurs personnels, d'ordinateurs portables et de tablettes fournis par le gouvernement. La plupart des utilisateurs proviennent d'EDSC et certains d'autres ministères du gouvernement du Canada et d'entités provinciales. L'Annexe C fournit des détails supplémentaires sur l'environnement technique actuel.

b) Dans son Plan ministériel de 2017-2018, EDSC a indiqué qu'il y a un risque que les renseignements personnels et de nature délicate d'EDSC puissent être consultés, utilisés, divulgués ou éliminés par inadvertance ou de façon inappropriée par des employés ou des tiers. Les stratégies de gestion des risques comprennent la mise en œuvre d'une stratégie

plus vaste de gestion des renseignements personnels et de nature délicate et l'examen des pratiques actuelles en matière de protection des renseignements personnels et de sécurité afin de protéger les renseignements personnels et de nature délicate. L'approche de réponse au risque comprend également l'utilisation de technologies (en plus des contrôles, des processus, des politiques et des ressources) pour appuyer la surveillance, la détection, l'analyse et l'enquête sur l'accès interne inapproprié ou la mauvaise utilisation de l'information sur les applications d'entreprise.

3. Description de la solution souhaitée et de la vision d'avenir

a) EDSC étudie les offres du marché pour surveiller et analyser les activités sur les applications d'entreprise afin de détecter et de gérer les incidents possibles d'accès interne ou d'utilisation inappropriée de l'information. Au départ, le Ministère aimerait installer la solution sur deux ou trois grandes applications internes, personnalisées et d'entreprise. Il prévoit ensuite adopter une approche fondée sur le risque afin d'élargir la technologie et la capacité qu'elle offre à d'autres applications d'entreprise. Comme on s'attend à ce que la solution logicielle évolue et mûrisse au fil du temps, EDSC s'attend à ce qu'elle continue d'être accessible, utilisée et développée sans interruption tout au long de sa durée de vie.

b) Le Canada se réserve le droit, à une date ultérieure et à sa seule discrétion, d'identifier la solution comme une solution pluriministérielle ou de la désigner comme une norme pangouvernementale du gouvernement du Canada si le Conseil d'examen de l'architecture intégrée du gouvernement du Canada le juge nécessaire.

c) En fonction des besoins du Ministère, EDSC étudie les **technologies gestion des incidents et de l'information de sécurité (GIIS)** ou de **surveillance des employés (SE)** pour gérer ce risque. Le Ministère cherche une solution qui permet d'effectuer ce qui suit :

i. Surveiller les applications spécifiées et détecter les incidents d'accès inapproprié à l'information en utilisant a) des règles opérationnelles définies et b) des capacités d'analyse avancées pour signaler les incidents potentiels indépendamment des règles opérationnelles prédéfinies pour les utilisateurs accédant aux applications d'entreprise.
ii. Utiliser un large éventail de sources de données (comme des fichiers journaux, y compris des journaux d'événements du système d'exploitation, des dossiers de base de données, des fichiers plats, des API propres aux fournisseurs, des sources fondées sur l'infonuagique/SaaS, etc.) pour détecter les cas possibles d'utilisation abusive et répréhensible de l'information lorsque les utilisateurs effectuent des transactions.
iii. Effectuer une analyse centrée sur l'utilisateur qui signale les incidents potentiels en fonction de l'activité ou du comportement de l'utilisateur et de l'information provenant des appareils, des applications et des sources d'information, afin qu'ils puissent faire l'objet d'une enquête.
iv. Surveiller et détecter les incidents potentiels indépendamment de l'utilisation de fichiers journaux pour reconnaître les tendances dans le comportement des utilisateurs avec les applications d'entreprise.

v. Produire des preuves irréfutables faciles à examiner et à comprendre par les enquêteurs et les gestionnaires de service pour confirmer si l'accès à l'information ou l'utilisation de l'information a été inapproprié.
vi. Prendre automatiquement des mesures définies en fonction de déclencheurs (p. ex., notifications automatiques aux utilisateurs de comportements potentiellement inappropriés) à l'appui de l'efficacité opérationnelle et de l'efficacité des enquêtes.
vii. Classifier les incidents pour permettre le triage des incidents en fonction du niveau de risque afin de soutenir l'efficacité, les flux de travail et les charges de travail pour les enquêteurs.
viii. S'intégrer aux solutions de gestion de cas existantes utilisées à EDSC (ou la solution offre des capacités de gestion de cas qui peuvent être utilisées à grande échelle par le Ministère). EDSC a mis en place un système de gestion des cas.
ix. Offrir des services gérés pour appuyer la préparation opérationnelle, la mise en œuvre, la configuration et l'intégration des applications d'EDSC. La solution est aussi accompagnée de services de soutien et de formation. EDSC doit être en mesure de mettre en œuvre la solution rapidement et d'examiner les considérations opérationnelles et les options à l'appui d'un logiciel ou d'un service.
x. Garantir la résidence des données au Canada, offrir des capacités bilingues en français et en anglais et satisfaire aux exigences du gouvernement du Canada en matière d'accessibilité. Les données doivent résider au Canada et sont protégées B.
xi. Offrir la possibilité d'être mise à profit par d'autres ministères, organismes et sociétés d'État du gouvernement du Canada ou des entités d'État provinciales.

4. Volume prévu

Métrique	Mise en œuvre initiale	État futur potentiel
Nombre d'applications d'entreprise à surveiller	4	130
Nombre d'utilisateurs d'applications d'entreprise à surveiller	13,100	25 000
Nombre d'utilisateurs simultanés	5,600	TBD
Volume de la transaction/par année	107,010,000	TBD

ANNEXE A : QUESTIONS ADRESSÉES À L'INDUSTRIE

Les répondants doivent fournir une réponse détaillée à chacune des questions suivantes :

Profil de l'entreprise	
A1	**Présence au Canada :** Avez-vous des bureaux au Canada?
A2	**Expérience pertinente – Accès à l'information :** Quel est le nombre de mises en œuvre actives et achevées à une échelle et à une complexité comparables à celles de notre organisation? Veuillez fournir la correspondance la plus proche avec les exigences comparables en ce qui a trait à l'industrie, à l'échelle, à la géographie et à la localisation, à la complexité et aux besoins en matière de conformité réglementaire. Quelles sont les pratiques exemplaires qui peuvent être mises à profit à partir de ces expériences?
A3	**Expérience et connaissances pertinentes – Gouvernement du Canada –** Votre entreprise a-t-elle de l'expérience pertinente, actuelle ou passée, auprès d'autres ministères fédéraux au sein du gouvernement du Canada, des gouvernements provinciaux du Canada ou de tout grand ministère fédéral dans d'autres administrations? Veuillez donner quelques exemples.
A4	**Viabilité financière :** Veuillez fournir des renseignements qui résument votre rendement récent en ce qui a trait aux revenus des nouvelles licences de logiciels, au taux de rétention des clients, à la rentabilité, aux dépenses et aux priorités en R-D, ainsi que d'autres renseignements qui, selon vous, aideraient EDSC à comprendre votre santé financière et votre viabilité financière.
A5	**Sécurité de l'entreprise :** Veuillez montrer comment vous vous conformez aux normes actuelles du gouvernement du Canada mentionnées à l'Annexe B. Veuillez indiquer si vous avez été assujetti à l'exigence de sécurité figurant à l'Annexe B en fournissant des noms de ministères ou d'organismes qui utilisent votre solution à titre de références.
A6	**Feuille de route des produits :** Veuillez décrire la vision et la feuille de route des produits de votre entreprise en ce qui a trait à la surveillance de l'utilisation de l'information et de l'accès aux applications d'entreprise par les employés, en précisant ce qui distingue votre solution proposée de la concurrence.
A7	**Stratégie relative aux services :** Veuillez décrire les services que vous offrez à vos clients en ce qui a trait à la surveillance de l'utilisation et de l'accès à l'information par les employés dans les offres d'applications d'entreprise avec des détails précis sur les partenariats ou d'autres approches de marché.
A8	**Références de clients :** Veuillez fournir trois références pour des clients comparables pour lesquels vous avez mis en œuvre une solution de contrôle de l'utilisation abusive de l'information de nature semblable. Au moins un client du secteur public canadien de

	préférence

Questions sur les produits – Aspect fonctionnel	
B1	**Surveillance des activités des employés et de l'accès à l'information sur les applications d'entreprise –** Veuillez décrire les capacités de votre produit à surveiller et à détecter l'accès interne et l'utilisation inappropriées de l'information dans les applications d'entreprise personnalisées. De quel type de technologie s'agit-il (gestion des incidents et de l'information de sécurité [GIIS], surveillance des employés [SE], etc.)?
B2	**Méthode de surveillance de l'activité dans l'application –** Comment le produit surveille-t-il l'utilisation de l'application et l'accès aux renseignements qu'elle contient? À quel niveau le produit exerce-y-il la surveillance (terminal, serveur, réseau) et que surveille-t-il exactement (activité de l'écran de l'application sur le terminal, fichiers journaux de l'application, etc.)? Cette surveillance dépend-elle d'intégrations à l'application ou à la base de données? Produit-il un enregistrement de l'activité de l'utilisateur dans l'application ou dépend-il d'une autre source d'information à cette fin (p. ex., fichier journal de l'application)? S'il faut un enregistrement de l'activité de l'utilisateur de l'application (p. ex., fichier journal de l'application), quels renseignements sont requis dans ces fichiers?
B3	**Sensibilité à la détection et faux positifs –** Veuillez décrire l'augmentation moyenne du nombre de cas vérifiés d'accès inapproprié, d'utilisation inappropriée de l'information ou de fraude interne après la mise en œuvre de votre solution dans des environnements semblables à ceux d'EDSC. Quel type de faux positifs, en moyenne, est observé avec votre produit au départ et après une période de « mise au point »? Quelles sont les capacités du produit de réduire le taux de faux positifs?
B4	**Sources de données supplémentaires –** Quels types de sources de données peuvent être ingérées ou le sont généralement, par le produit pour enrichir la capacité de détection? Par exemple, peut-il utiliser des données provenant des plateformes de RH (p. ex., PeopleSoft), des données d'accès aux immeubles et des fichiers et de l'information des logiciels de sécurité de l'information? Décrire les sources à partir desquelles il peut recueillir des données (p. ex., fichiers journaux, journaux d'événements du système d'exploitation, dossiers de base de données, fichiers plats, API propres au fournisseur, sources fondées sur l'infonuagique/SaaS, etc.) et la façon dont la collecte des données est réalisée.
B5	**Détection fondée sur des règles opérationnelles –** Le produit permet-il de détecter des incidents potentiels en fonction de règles opérationnelles? Veuillez décrire comment ces règles sont définies et « codées » et quels ensembles de compétences sont

Questions sur les produits – Aspect fonctionnel	
	nécessaires pour les définir et les mettre en œuvre. Veuillez décrire la nature de ces règles opérationnelles et donner une estimation du soutien dont vous avez besoin de la part d'EDSC pour les définir?
B6	**Détection avancée indépendante des règles opérationnelles –** Votre solution offre-t-elle des capacités analytiques avancées (apprentissage automatique, etc.) pour surveiller et signaler les incidents en fonction des modèles de comportement des utilisateurs, indépendamment des règles opérationnelles définies? Décrivez en détail comment ces capacités fonctionnent, quels renseignements sont nécessaires, comment le système doit être entraîné à cette fin, combien de temps prend cet entraînement et quelles sont les compétences nécessaires pour entraîner le système.
B7	**Détection avancée du comportement de l'utilisateur dans l'ensemble des appareils et des applications –** Votre solution a-t-elle des capacités d'analyse des comportements des utilisateurs et des entités (ACUE) ou d'analyse avancée (apprentissage machine, etc.) pour surveiller et signaler les incidents en fonction des tendances dans le comportement de l'utilisateur sur l'ensemble des appareils, des applications et des périodes? Veuillez décrire ces capacités en détail. Comment le produit attribue-t-il les incidents à des personnes précises (utilisateurs par rapport à des appareils)?
B8	**Mise au point du produit –** Veuillez décrire si et comment le produit doit être configuré, ajusté ou entraîné pour optimiser la précision et l'efficacité de la détection. Combien de temps cette période de « raffinement » prendrait-elle habituellement? Quel type d'information est nécessaire? Quelles sont les exigences du client?
B9	**Collusion –** Le produit peut-il détecter la collusion entre plusieurs utilisateurs internes? Décrivez comment le produit s'y prend.
B10	**Automatisation –** Veuillez décrire toute capacité d'automatisation dans l'exécution d'actions personnalisées en réponse aux déclencheurs et au risque d'incident potentiel (p. ex., avertissement par courriel à la première occurrence d'un comportement potentiellement inapproprié). Comment ces actions automatisées sont-elles définies et configurées? Veuillez décrire la profondeur et l'étendue de ces capacités.
B11	**Catégorisation et classement des incidents par niveau de risque –** Le produit a-t-il la capacité de catégoriser ou de classer les incidents par niveau de risque (p. ex., criticité, volume, etc.). S'agit-il d'une capacité d'affectation automatisée ou manuelle? Veuillez décrire comment cela fonctionne.
B12	**Triage et gestion du flux de travail par risque –** Veuillez décrire les capacités de triage et de gestion du volume d'incidents possibles en fonction du risque. Est-ce que cette fonction est manuelle ou automatisée? Veuillez en décrire le mode de

Questions sur les produits – Aspect fonctionnel	
	fonctionnement.
B13	**Preuve –** Veuillez décrire en détail le type de preuve que le produit génère pour les enquêteurs et les gestionnaires d'unité opérationnelle afin d'évaluer et de confirmer les incidents de mauvaise utilisation et d'utilisation abusive de l'information. S'agit-il d'une vidéo, d'une lecture de captures d'écran des actions des utilisateurs sur les applications en fonction des déclencheurs de détection? S'agit-il d'un rapport? Veuillez décrire cette fonction en détail.
B14	**Surveillance sélective –** Le client peut-il définir ce qui est surveillé (p. ex., surveiller es applications x et y, et non le courriel, l'activité sur le Web, etc.)?
B15	**Analyse –** Au-delà des capacités analytiques utilisées pour la détection, veuillez décrire toute capacité analytique supplémentaire du produit.
B16	**Rapports –** Quel type d'information peut être intégrée dans un rapport à partir du système? Les rapports sont-ils configurables? Quel est le format des rapports? Votre produit comporte-t-il des modules d'extension pour les plateformes et les applications communes de renseignement d'entreprise?
B17	**Rapidité –** Quel est le délai entre le moment où un incident se produit et celui où une alerte est générée? Votre solution offre-t-elle une détection en temps réel? Le traitement par lots en dehors des heures de travail?
B18	**Gestion des cas –** Ce système peut-il appuyer la gestion des cas? Peut-il être intégré à d'autres systèmes qui soutiennent la gestion des cas et des flux de travail?
C1	**Nombre d'applications :** Quel est le nombre total d'applications d'entreprise que le produit peut surveiller? Décrivez comment vous offrez l'extensibilité de la solution. Quel est le plus grand nombre d'applications surveillées, pour une même organisation?
C2	**Nombre d'utilisateurs :** Combien d'utilisateurs totaux peuvent être surveillés par le système? Combien d'utilisateurs peuvent être surveillés simultanément? Quel est le plus grand nombre d'utilisateurs surveillés, pour une même organisation?
C3	**Volume de transactions :** Quelle est la fourchette (minimum, maximum) de volume de transactions que peut prendre en charge votre solution? À quel niveau de volume de transactions le rendement de la solution est-il affecté négativement?
C4	**Déploiement :** Le produit est-il déployé sur des dispositifs terminaux ou fonctionne-t-il sur un serveur central? Où l'information est-elle générée (terminal?) et où l'information est-elle stockée?

Questions sur les produits – Aspect fonctionnel	
C5	**Largeur de bande interne du réseau :** Selon les paramètres de volume de l'utilisateur et de l'application, quelles seraient les exigences internes en matière de bande passante du réseau? Quelle charge/tension la solution imposerait-elle au réseau interne?
C6	**Stockage :** Selon les paramètres de volume de l'utilisateur et de l'application fournis, quelle quantité de stockage serait nécessaire?
C7	**Dispositifs –** Sur quels appareils le produit peut-il surveiller l'activité des applications d'entreprise par les utilisateurs internes (ordinateurs personnels, tablettes, téléphones intelligents, etc.)
C8	**Configuration de l'utilisateur :** Veuillez décrire le niveau de configuration disponible – ce qui peut être configuré et comment? Peut-il être configuré par le client indépendamment de votre entreprise? Quel est le niveau d'expertise requis pour configurer le système? Quelles parties de la solution doivent être configuré es conjointement avec votre entreprise ou uniquement par elle?
C9	**Personnalisation :** Quelles parties de la solution peuvent ou devraient être personnalisées pour répondre aux besoins des clients? Le client peut-il personnaliser certains éléments de la solution au-delà des options de configuration intégrées?
C10	**En nuage/sur place :** Votre solution est-elle offerte sur place, en nuage, en logiciel en tant que service (SaaS) ou s'agit-il d'un service géré? Certaines des données associées à votre solution sont-elles stockées dans le nuage? Si oui, préciser le nom et l'emplacement du fournisseur de services en nuage? Certaines des données associées à votre solution sont-elles stockées à l'extérieur du Canada? Si oui, où?
C11	**Connecteurs/Intégration aux applications de sécurité de l'information :** Veuillez décrire les types et les fournisseurs de logiciels de sécurité de l'information auxquels votre produit peut se connecter. Comment cela fonctionne-t-il avec ces produits (Transferts de fichiers? Modules d'extension? Intégrations figées dans le code?). Exemples : logiciel de contrôle d'accès, authentifiants, logiciel de surveillance des terminaux, logiciel de surveillance de la PD, etc.
C12	**Accessibilité :** Votre solution respecte-t-elle les exigences du gouvernement du Canada en matière d'accessibilité, y compris la Boîte à outils de l'expérience Web (BOEW) et les Règles pour l'accessibilité des contenus Web (WCAG 2.0AA) (Référence : BOEW et WCAG 2.0AA)?
C13	**Bilingue :** Votre solution appuie-t-elle la norme de bilinguisme du GC en vertu de la *Loi sur les langues officielles* (français et anglais)?
C14	**CATS :** Votre solution est-elle conforme aux spécifications des Solutions technologiques

Questions sur les produits – Aspect fonctionnel	
	d'authentification électronique (STAE) version 2.0? Offre-t-elle la souplesse nécessaire pour s'adapter aux versions futures des spécifications des STAE?

Questions sur le produit – Sécurité de l'information et architecture	
E1	**Connecteurs/Intégration aux applications de sécurité de l'information :** Veuillez décrire les types et les fournisseurs de logiciels de sécurité de l'information auxquels votre produit peut se connecter. Comment cela fonctionne-t-il avec ces produits (Transferts de fichiers? Modules d'extension? Intégrations figées dans le code?). Exemples : logiciel de contrôle d'accès, authentifiants, logiciel de surveillance des terminaux, logiciel de surveillance de la PD, etc.
E2	**Plateformes prises en charge :** Quelles plateformes informatiques votre solution prend-elle en charge? Veuillez préciser le SE du serveur et les navigateurs pris en charge (pour tous les types d'appareils).
E3	**Accès :** Décrire le niveau d'accès des clients aux outils de développement et de collaboration du fournisseur (p. ex., dépôt de code source, intégration continue et outils de mise à l'essai automatisés, modules d'extension, etc.).
E4	**Langage de programmation :** Quel langage de programmation a été utilisé pour développer votre application? Le logiciel est-il rédigé dans un langage de développement disponible sur le marché qui est encore amélioré et soutenu par le fournisseur?
E5	**Aperçu de l'architecture :** Veuillez donner un aperçu de l'architecture de vos solutions.
E6	**Protection des renseignements :** Comment votre solution protège-t-elle les renseignements confidentiels qu'elle recueille, stocke ou transmet (p. ex., Protégé B, détails d'enquête, etc.) pour assurer un haut degré d'intégrité de l'information?
E7	**Administration :** Veuillez décrire les fonctions administratives de votre solution (p. ex., gestion de compte, contrôle d'accès, journalisation, intrusion, alertes, etc.).
E8	**Attestations de sécurité :** Votre solution comporte-t-elle des attestations ou des évaluations de sécurité?
E9	**Récupération après sinistre :** Décrivez votre méthode de reprise après sinistre et de continuité des activités pour les éléments suivants : • Votre propre plateforme de produits ou de services, si elle est offerte comme solution infonuagique externe.

Questions sur le produit – Sécurité de l'information et architecture	
	• Données ou biens de PI propres au client qui font partie de la portée des services fournis?

Mise en œuvre, formation, soutien et services gérés	
F1	**Évaluation de l'état de préparation :** Veuillez décrire les mesures prises pour évaluer l'état de préparation d'un client et l'aider à adopter votre solution. Quelles sont les composantes de l'évaluation? De quoi le client a-t-il besoin (sur les plans technique et opérationnel) avant la mise en œuvre?
F2	**Étapes de mise en œuvre :** Veuillez décrire les étapes à suivre pour mettre en œuvre votre solution. En supposant que l'infrastructure de TI était en place, combien de temps faudrait-il à votre personnel pour installer votre système, le configurer et le préparer à la production? En règle générale, combien de temps faut-il à un client pour terminer ce travail lui-même, avec et sans soutien technique?
F3	**Méthodologie de mise en œuvre :** Veuillez décrire votre méthodologie, y compris les outils et les processus à utiliser pour une mise en œuvre réussie. Décrire les processus à l'appui des essais d'acceptation, des essais d'interopérabilité et d'intégration, des essais de rendement, des essais de sécurité et de migration et de l'expertise en la matière qui seraient disponibles pour appuyer la mise en œuvre.
F4	**Risques liés à la mise en œuvre :** Quels sont les risques typiques liés à la mise en œuvre dans le cadre d'autres projets de taille et de portée semblables? Quelles mesures avez-vous prises pour réduire au minimum ces risques?
F5	**Mise à l'essai :** Quel est votre rôle habituel dans les phases de mise à l'essai, de gestion des versions et de maintenance?
F6	**Transition vers l'acceptation :** Comment le fournisseur appuierait-il EDSC pendant la transition de la « mise en service » à l'« acceptation finale »?
F7	**Services de tiers :** Veuillez indiquer si des services de tiers sont requis pour la mise en œuvre et le soutien. Ces ressources relèvent-elles habituellement du client (EDSC) ou du fournisseur?
F8	**Services de mise en œuvre :** Quels services votre entreprise offre-t-elle pour appuyer la mise en œuvre du produit?

Mise en œuvre, formation, soutien et services gérés	
F9	**Services de « formation » liés à la configuration et à la solution :** Quels services votre entreprise offre-t-elle pour configurer la solution, y compris la configuration initiale, le codage des règles opérationnelles, l'élaboration des règles opérationnelles, l'« entraînement » ou la mise au point de la solution, la production de rapports, etc.?
F10	**Services d'intégration :** Quels services votre entreprise offre-t-elle pour appuyer les intégrations et les connexions nécessaires à d'autres plateformes logicielles?
F11	**Formation :** Quelle formation sur le produit est offerte avant et après l'installation? Offrez-vous de la formation, des manuels d'utilisation et du soutien en français et en anglais? Comment la formation est-elle adaptée et offerte à différents types d'utilisateurs, notamment les utilisateurs administratifs (TI et sécurité de l'information), les super-utilisateurs, les enquêteurs, les utilisateurs finaux, les gestionnaires d'unité opérationnelle, le personnel d'analyse, etc.
F12	**Ressources et activités des clients :** Quelles activités et quels types et niveaux de ressources d'EDSC seraient nécessaires pour mettre en œuvre votre solution standard?
F13	**Modèle de soutien :** Veuillez décrire votre modèle de maintenance et de soutien et ce qui est inclus (p. ex., soutien sur place ou à distance, heures d'ouverture, soutien linguistique, temps d'intervention selon le niveau d'incident ou de problème, etc.). Comment rendez-vous compte de votre rendement (sur une base quotidienne, hebdomadaire ou mensuelle) quant au traitement des demandes de soutien?
F14	**Ressources de soutien d'EDSC :** Quelles sont les activités et le type/niveau d'expertise en ressources dont EDSC aurait besoin pour maintenir votre solution de façon continue?
F15	**Gestion des versions :** À quelle fréquence publiez-vous une nouvelle version? Quelle est votre stratégie de gestion des versions? Combien de temps faut-il, en moyenne, pour mettre en œuvre une nouvelle version? Combien de versions appuyez-vous? (p. ex., la version actuelle est-elle la seule prise en charge, ou les versions précédentes sont-elles également prises en charge?) Pendant combien de temps une version est-elle prise en charge, après la publication d'une nouvelle version? (p. ex., le soutien de la version actuelle expire-t-il dès que la prochaine version est publiée?) Combien de temps à l'avance annoncez-vous normalement une version en fin de vie?
F16	**Gestion des correctifs :** Quelle est votre stratégie de gestion des correctifs? Combien de temps faut-il, en moyenne, pour mettre en œuvre les correctifs? Quel est l'effort requis en termes de ressources et de coûts?
F17	**Communication :** Comment informez-vous vos clients des nouvelles versions et des mises à niveau critiques? Comment rendez-vous compte de votre rendement (sur une

Mise en œuvre, formation, soutien et services gérés	
	base quotidienne, hebdomadaire ou mensuelle) quant au traitement des demandes de soutien?
F18	**Gestion des relations :** Comment serait généralement géré le soutien d'une organisation de la taille et de la complexité d'EDSC (p. ex., personnel de soutien spécialisé, centre d'appels, etc.)

Tarification et octroi de licences	
G1	**Distribution :** Distribuez-vous votre solution logicielle au Canada directement ou par l'entremise d'un tiers autorisé?
G2	**Modules :** Décrivez les modules fonctionnels (composants) inclus dans la solution de base et les modules fonctionnels (composants) supplémentaires disponibles.
G3	**Coûts :** Veuillez décrire les coûts de la solution de base et déterminer les coûts différentiels des options de solution qui sont des ajouts complémentaires pour améliorer la solution de base, y compris une description des volets et des catégories standards pour les services professionnels.
G4	Veuillez décrire les modèles de tarification de la solution et l'option que vous recommanderiez. Par exemple, votre modèle préféré est-il l'un des suivants : • achat du produit et des services de mise en œuvre auprès du fournisseur de la solution; • achat des licences et conclusion d'un contrat avec un partenaire de mise en œuvre; • achat du logiciel et achèvement de la mise en œuvre à l'aide du personnel interne d'EDSC ou y a-t-il une autre option que vous proposeriez, veuillez expliquer.
G5	Améliorations : Veuillez décrire le modèle de prix pour les améliorations, comme l'adaptation ou la modification de la solution après la mise en œuvre en fonction des commentaires du client.
G6	Modèle de licence : Veuillez décrire le modèle de licence de votre solution. Si votre solution est disponible dans une configuration de licence d'entreprise, veuillez décrire les conditions nécessaires pour être admissible à une licence d'entreprise, y compris tout investissement minimal en argent ou en autres licences.
G7	Expansion : Votre modèle de licence permet-il d'élargir la solution proposée à d'autres ministères ou organismes du gouvernement du Canada?

Tarification et octroi de licences	
G8	Veuillez indiquer une fourchette de prix annuels donnant un ordre de grandeur pour la solution et les services que vous avez fournis à une organisation comparable à EDSC. N'hésitez pas à formuler des hypothèses raisonnables au sujet de l'échelle et de la portée et à énoncer les principales hypothèses ayant une incidence sur le prix dans votre réponse.

ANNEXE B : EXIGENCES EN MATIÈRE DE SÉCURITÉ DES FOURNISSEURS

Un examen de sécurité détaillé doit être effectué pour déterminer les exigences de sécurité que devront satisfaire les fournisseurs retenus avant de travailler au projet. Les exigences de sécurité suivantes sont fournies à titre indicatif et peuvent être modifiées :

L'entrepreneur ou l'offrant doit en tout temps pendant l'exécution du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement détenir une attestation de vérification d'organisation désignée (VOD) valide et une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC).

CHAQUE membre du personnel de l'entrepreneur ou de l'offrant ayant accès à des renseignements, à des biens ou à des lieux de travail PROTÉGÉS doit détenir une COTE DE FIABILITÉ valide, délivrée ou approuvée par la DSIC de SPAC.

L'entrepreneur NE DOIT PAS utiliser ses systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS tant que la DSIC de SPAC ne lui en aura pas donné l'autorisation par écrit. Une fois l'autorisation accordée ou approuvée, les tâches peuvent être exécutées jusqu'au niveau PROTÉGÉ B, y compris un lien électronique jusqu'au niveau PROTÉGÉ B.

Des contrats de sous-traitance renfermant des exigences de sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de la DSIC de SPAC.

L'entrepreneur ou l'offrant doit respecter les dispositions :

de la Liste de vérification des exigences relatives à la sécurité et de la directive de sécurité (s'il y a lieu);

du Manuel de la sécurité industrielle (dernière édition).

Les fournisseurs ne seront pas tenus de se conformer à ces exigences aux fins de la présente demande de renseignements.

ANNEXE C : POLITIQUES DU CONSEIL DU TRÉSOR

Le fournisseur de services doit observer directement l'ensemble des politiques, directives et lignes directrices pertinentes, notamment :

Cadre stratégique pour l'information et la technologie
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12452&section=text

Politique sur la gestion de l'information
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742

Politique sur la gestion des technologies de l'information
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12755

Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328&section=text

Ligne directrice sur la définition des exigences en matière d'authentification
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262&section=text#sec1.2

Politique sur l'utilisation acceptable des dispositifs et des réseaux
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=27122

Les politiques, les normes et les directives qui régissent la prestation de services en ligne comprennent, entre autres, les suivantes : (ces normes Web remplacent la Normalisation des sites Internet 2.0)

Normes Web pour le gouvernement du Canada
http://www.tbs-sct.gc.ca/ws-nw/index-eng.asp

Norme sur l'accessibilité des sites Web
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

Norme sur la facilité d'emploi des sites Web
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=24227

Norme sur l'interopérabilité du Web
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=25875

Normes sur la normalisation des sites Internet, partie 4 : Norme sur le courriel
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=25439

Politique sur l'audit interne
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16484

Politique de communication du gouvernement du Canada
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12316

Politique sur le Programme de coordination de l'image de marque
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12314

Directive sur la gestion de l'identité
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577

Norme sur l'assurance de l'identité et des justificatifs
www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776

Politique sur la protection de la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510

Politique sur l'accès à l'information
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12453

Directive sur l'administration de la *Loi sur l'accès à l'information*
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18310

Politique sur la sécurité du gouvernement
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

Norme opérationnelle sur la sécurité matérielle
https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text

Politique sur la gouvernance en matière de gestion financière
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=14005

Norme sur la gestion des comptes de médias sociaux
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27033

D'autres politiques, normes, lignes directrices et directives sont consultables dans leur intégralité sur le site Web du Secrétariat du Conseil du Trésor du Canada www.tbs-sct.gc.ca.

ANNEXE D : PRINCIPES DE L'ARCHITECTURE D'ENTREPRISE

La solution du fournisseur de services doit être conforme aux principes suivants de l'architecture intégrée du gouvernement du Canada :

Portée : L'architecture intégrée du GC en premier, les groupements de l'architecture intégrée du GC en deuxième lieu et le caractère unique du ministère en dernier

Réutilisabilité : Réutiliser en premier, acheter en deuxième lieu, construire en dernier

Organisme et utilisateurs en premier

Souci du service à la clientèle

L'information, y compris les données, constitue un actif

Interopérabilité

Ouvert par défaut, exclusif seulement par nécessité

Mobilité préférée

Sécurité à dessein

Souci de la vie privée

Priorité à l'infonuagique

Gestion de la dette technologique