Canada Revenue Agency | Agence du revenu du Canada

RETURN BIDS TO : - RETOURNER LES SOUMISSIONS À:

Canada Revenue Agency
Agence du revenu du Canada
See herein / Voir dans ce document

Proposal to: Canada Revenue Agency
We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein and/or attached hereto, the goods and/or services listed herein and on any attached sheets at the price(s) set out therefor.

Proposition à : l'Agence du revenu du Canada
Nous offrons par la présente de vendre à Sa Majesté la Reine du Chef du Canada, en conformité avec les conditions énoncées dans la présente incluses par référence dans la présente et/ou incluses par référence aux annexes jointes à la présente et ci-jointes, les biens et/ou services énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Bidder's Legal Name and Address - (ensure the Bidder's complete legal name is properly set out)
Raison sociale et adresse du Soumissionnaire - (s'assurer que le nom légal au complet du soumissionnaire est correctement indiqué)

_____

_____

_____

Bidder is required to identify below the name and title of the individual authorized to sign on behalf of the Bidder – Soumissionnaire doit identifier ci-bas le nom et le titre de la personne autorisée à signer au nom du soumissionnaire

_____
Name /Nom

_____
Title/Titre

_____
Signature

_____
Date (yyyy-mm-dd)/(aaaa-mm-jj)

(____)_____
Telephone No. – No de téléphone
(____)_____
Fax No. – No de télécopieur

_____
E-mail address – Adresse de courriel

AMENDMENT TO REQUEST FOR PROPOSAL / MODIFICATION DE DEMANDE DE PROPOSITION

Title – Sujet

Lignes anonymes de signalement de la fraude interne et de l'utilisation malveillante de l'ARC

Solicitation No. – No de l'invitation	**Date (yyyy-mm-dd) (aaaa-mm-jj)**
1000318737/A	2015-01-08

Amendment No. - N° modif.

002

Solicitation closes – L'invitation prend fin on – le	**Time zone – Fuseau horaire**
2015-01-21 **(yyyy-mm-dd) (aaaa-mm-jj) at – à 2:00 P.M. / 14 h**	EST /HNE Eastern Standard Time/ Heure Normale de l'Est

Contracting Authority – Autorité contractante

Name – Nom Phuong Ly

Address – Adresse - See original document/ voir document original

E-mail address – Adresse de courriel – Phuong.Ly@cra-arc.gc.ca

Telephone No. – No de téléphone
(613) 957-3291

Fax No. – No de télécopieur
(613) 957-6655

Destination - Destination

See herein / Voir dans ce document

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT.

LE PRÉSENT DOCUMENT COMPORTE UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ.

MODIFICATION n° 002 À LA DEMANDE DE SOUMISSIONS

La modification à cette demande de soumissions est émise aux fins suivantes :
1. Répondre aux questions suivantes soumises durant la période de soumissions, conformément à la DDP; et
2. Modifier la DDP.

1. QUESTIONS ET RÉPONSES

Q10. Comme la date limite pour les réponses est la semaine prochaine, et que vos réponses peuvent nous amener à modifier nos réponses, nous aimerions les recevoir le plus rapidement possible. OU serait-il possible de recevoir une courte extension pour soumettre la soumission? Est-ce que la date de clôture peut être prolonge jusqu'au 31 janvier?

R10. L'ARC n'est pas en accord de reporter la date de clôture au 31 janvier 2015, mais la date de clôture des soumissions a été changée au 21 janvier 2015. Prière de référer à la modification O3 ci-dessous.

Q11. Est-ce l'ARC accepterait une stratégie de tarification alternative au lieu d'un coût fixe mensuel.

R11. L'ARC demande un taux fixe mensuel tout compris de sorte que toutes les propositions financières peuvent être évaluées de façon uniforme et équitable.

Q12. Est-ce que l'ARC peut nous fournir le nombre d'allégations soumises reçues dans les dernières trois années?

R12. Comme l'ARC ne dispose pas actuellement de système de dénonciation anonyme formelle en place, nous ne sommes pas en mesure de fournir le nombre d'allégations soumises reçues.

Q13. Est-ce que l'ARC serait prête à supprimer l'exigence pour l'entrepreneur d'omettre le nom de la source et toute information personnelle/identifiable du rapport d'allégations?

R13. Oui. Toutefois, l'entrepreneur doit fournir des avertissements et des rappels à la source de ne pas s'auto-identifier ni de fournir aucune information personnelle/identifiable. Veuillez-vous référer aux modifications O4 et O5.

Q14. Dans la liste des exigences obligatoires, à l'occasion, notre entreprise comporte des processus plus rigoureux que ceux qui sont demandés par l'ARC (par exemple, les renouvellements de mot de passe sont exigés plus fréquemment qu'à tous les 180 jours, ou l'utilisation d'un chiffrement cryptographique plus récent et/ou plus sécurisé). Si l'ARC estime que ces exigences sont trop rigoureuses, pouvez-vous confirmer que dans ces circonstances, l'exigence sera notée comme « respectée », pourvu que nous précisions dans notre réponse que l'exigence de base est respectée?

R14. Oui. L'ARC acceptera des configurations de sécurité plus rigoureuses. Conformément à la « PARTIE 3 – DIRECTIVES SUR LA PRÉPARATION DE LA SOUMISSION » (page 12 de 66), le soumissionnaire doit fournir suffisamment de renseignements qui démontrent comment elles répondent ou dépassent l'exigence énoncée.

Q15. Dans la liste des exigences obligatoires, à l'occasion, notre entreprise comporte des processus qui font en sorte qu'une exigence ne s'applique pas (c.-à-d. les renseignements au niveau Protégé B ne sont pas stockés sur des dispositifs miniatures de stockage électronique). Si l'ARC estime que ces exigences ne s'appliquent pas, pouvez-vous confirmer que dans ces circonstances, l'exigence sera notée comme « respectée »?

R15. Oui. Toutefois, le fournisseur doit tout de même fournir une explication adéquate des raisons pour lesquelles l'exigence ne s'applique pas ou de la façon dont les risques à la sécurité connexes doivent être atténués. Le

soumissionnaire doit fournir suffisamment de détails pour que l'ARC puisse déterminer s'il respecte l'exigence de l'ARC.

Conformément à la section 2.1 (Exigences obligatoires), toutes les exigences obligatoires doivent être respectées. Dans l'exemple fourni dans la question, le soumissionnaire doit indiquer comment il gère le cycle de vie des dispositifs miniatures de stockage électronique afin de s'assurer que les renseignements de nature délicate sont protégés.

Q16 A. AC-2 a) À qui « l'organisation » fait-elle référence dans cette question (l'ARC ou le soumissionnaire)? Si le personnel administratif d'un soumissionnaire fournit un soutien administratif et des comptes au personnel de l'ARC désigné par l'ARC (pour assurer l'intégrité du système), est-ce acceptable pour l'ARC?

R16 A. « L'organisation » renvoie au soumissionnaire. L'ARC exige que le soumissionnaire fournisse suffisamment de renseignements qui indiquent que les pratiques exemplaires pour la gestion de comptes et les privilèges de compte sont appliquées dans l'organisation du soumissionnaire, ce qui comprend la gestion de tous les comptes d'utilisateur, des comptes d'administration internes de la TI aux comptes des clients de l'ARC. La suggestion du soumissionnaire ci-dessus donnera un certain contexte pour une réponse acceptable. Veuillez consulter les Conseils supplémentaires à la section AC-2, au lien suivant : {https://www.cse-cst.gc.ca/fr/node/265/html/22840}.

Q16 B. Si le personnel administratif du soumissionnaire établit des comptes d'utilisateur pour différentes catégories d'utilisateurs dans sa fonction requise à la demande du client, est-ce considéré acceptable par l'ARC?

R16 B. Cela répondra à une partie de l'exigence. Le soumissionnaire doit aussi fournir des renseignements supplémentaires qui indiquent que les pratiques exemplaires sont suivies pour fournir une participation en groupe aux employés internes du soumissionnaire, ce qui comprend l'accès à différents groupes d'utilisateurs, p. ex. l'administration de systèmes, l'administration d'applications, l'administration du système de gestion de base de données (SGBD), le personnel de bureau, entre autres.

Q16 C. j) Sur quels critères l'examen du compte tous les 30 jours serait-il fondé? Quel devrait être le format d'un tel examen?

R16 C. Cette exigence renvoie à la pratique visant à examiner périodiquement tous les comptes d'utilisateur afin de s'assurer que les comptes d'utilisateur ne comportent que des privilèges d'accès autorisés, que les comptes inutilisés sont adéquatement suspendus ou supprimés, entre autres. L'ARC cherche à obtenir la confirmation que le soumissionnaire suit de telles pratiques pour les comptes d'employé et de client. L'organisation de chaque soumissionnaire décide des critères et du format, selon ses processus de sécurité internes.

Q17. AC-11 a) Un délai d'inactivité de 15 minutes établi pour un rapporteur qui présente un signalement et un délai d'inactivité de deux heures accordé pour les agents de ligne directe, puisqu'ils remplissent le signalement par téléphone, sont-ils acceptables pour l'ARC?

R17. Sur le plan de la sécurité, les délais d'inactivité proposés sont acceptables. Prière de référer à la modification O5 ci-dessous.

Q18. AU-2 a) Si le soumissionnaire tient à jour un journal de bord des activités d'entretien de la base de données et recycle ce journal tous les sept jours, est-ce acceptable pour l'ARC?

R18. Selon l'exigence « (A) L'organisation doit être en mesure de vérifier les événements suivants : accès de l'administrateur de système et de l'utilisateur général aux applications, activités de maintenance des bases de données et changements de configuration des systèmes ». Pour répondre à cette exigence, le soumissionnaire doit aussi être en mesure d'enregistrer l'accès de l'administrateur de système ou de l'utilisateur général aux applications et aux changements de configuration de système.

De plus, conformément à l'exigence AU-11, « (A) L'organisation conserve les enregistrements de vérification pour la durée du contrat, ou autrement indiqué par l'ARC pour soutenir les enquêtes après coup sur les incidents de sécurité et satisfaire aux exigences réglementaires et organisationnelles de conservation de l'information ». Par conséquent, la période de conservation de sept jours n'est pas suffisante pour répondre à l'exigence AU-11.

Q19. AU-5 b) Le soumissionnaire a des limites d'espace disque qui envoient des alertes afin qu'elles puissent être traitées à plusieurs seuils avant qu'une telle défaillance se produise, ce qui élimine la nécessité d'un système de vérification pour arrêter le système d'information ou écraser les enregistrements de vérification. Est-ce acceptable pour l'ARC?

R18. Oui, à condition que la solution proposée continue de respecter les autres exigences en matière de vérification figurant aux pages 56 et 57, à la section Vérification et responsabilisation.

Q20. AU-11 a) Veuillez préciser les durées de conservation des enregistrements de vérification requises pour chaque type d'enregistrements de vérification.

R20. Les durées de conservation des enregistrements de vérification requises sont de quatre ans plus l'année en cours pour chacun des éléments suivants :

- l'accès de l'administrateur de système ou de l'utilisateur général aux applications;
- les activités d'entretien des bases de données;
- les changements de configuration du système.

Q21. IA-5 e) Est-ce que l'ARC examinerait la possibilité d'interdire la réutilisation des mots de passe pendant trois générations, plutôt que 10?

R21. Oui, l'ARC acceptera l'interdiction de la réutilisation des mots de passe pendant trois générations. Prière de référer à la modification O5 ci-dessous.

Q22. SC-12 et SC-13, la DDP nécessite qu'une partie de la solution soit un site Web. Cela exige un service Web HTTPS. La documentation de la DDP nécessite que l'organisation produise, contrôle et distribue des clés cryptographiques symétriques et asymétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC, et qu'elle utilise une cryptographie approuvée par le CSTC pour protéger les données classifiées. Cependant, l'obtention d'un service Web nécessite un paradigme différent de celui qui est décrit dans la documentation. Pour tout service Web HTTPS, certaines suites de chiffres sont requises pour combiner le protocole, l'échange de clés, l'algorithme de signature numérique, l'algorithme de cryptographie symétrique et l'algorithme de hachage, ainsi que leurs forces de chiffre binaire respectives. Afin de permettre un accès à différents navigateurs, il est nécessaire de soutenir de multiples suites de ce genre. De plus, choisir l'ensemble adéquat de suites est la clé pour fournir un niveau de sécurité maximum, tout en permettant des connections pour un éventail de navigateurs. Dans la documentation fournie, il est difficile de déterminer les suites qui seraient acceptables pour l'ARC. Veuillez nous fournir une liste des suites de chiffres que l'ARC approuve.

R22. L'ARC acceptera les protocoles et les suites de chiffres compatibles qui répondent aux conseils fournis dans les documents ITSB-60 (https://www.cse-cst.gc.ca/fr/node/253/html/15204) et ITSA-11E (https://www.cse-cst.gc.ca/fr/node/227/html/15164) du CSTC. Le soumissionnaire a la souplesse d'ajuster la liste des protocoles et des suites de chiffres pris en charge afin de tenir à jour les navigateurs grand public, tout en respectant les normes du CSTC. Par exemple, les navigateurs largement utilisés tels qu'Internet Explorer, Chrome, Firefox, Safari et Opera prennent en charge le protocole TLS 1.0/1.1/1.2, tel qu'il est exigé par le document ITSB-60, et les suites de chiffres qui utilisent l'algorithme SHA-256, tel qu'il est indiqué dans le document ITSA-11E. Prière de référer à la modification O5 ci-dessous.

2. MODIFICATIONS À LA DDP

O3. Sur la page couverture de la demande de proposition – L'invitation prend fin on – le :

Supprimer

2015-01-14

Insérer

2015-01-21

O4. À l'annexe A-1 : EXIGENCES OPÉRATIONNELLES, section 1.0 TÂCHES, sous-section 1.1 Services requis

Supprimer

- Assurer l'anonymat de la source en tout temps (l'entrepreneur ne doit pas enregistrer le nom de la source en aucun temps même s'il est fourni);

Insérer

- Assurer l'anonymat de la source en fournissant des avertissements et des rappels à la source de ne pas fournir aucune information personnelle/identifiable;

O5. À l'annexe A-3 : EXIGENCES EN MATIERE DE SECURITE DES TECHNOLOGIES DE L'INFORMATION

Supprimer :

AC-11	VERROUILLAGE DE SESSION	(A) Le système d'information empêche tout autre accès au système en verrouillant la session après un délai d'inactivité déterminé par l'ARC ou à la réception d'une demande d'un utilisateur. (B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur réinitialise l'accès en exécutant les procédures établies d'identification et d'authentification.

Et

AU-9	PROTECTION DE L'INFORMATION DE VÉRIFICATION	(A) Le système d'information protège l'information de vérification et les outils de vérification contre l'accès, la modification et la suppression non autorisés. À l'exception d'omettre le nom et toutes particularités de la Source.

Et

IA-5	GESTION DES AUTHENTIFIANTS	Authentification axée sur les mots de passe – Le système d'information : (a) applique un mot de passe de complexité minimale d'une combinaison de lettres majuscules et minuscules, des numéros et des symboles (p. ex., @, #, $, %); (c) chiffre les mots de passe stockés et en transit; (d) applique les restrictions minimales et maximales de durée des mots de passe, soit 180 jours ou moins; et (e) interdit la réutilisation des mots de passe pendant 10 générations.

Et

SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES	L'organisation produit, contrôle et distribue des clés cryptographiques symétriques et asymétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC (https://www.cse-cst.gc.ca/fr/publication/itsa-11e).
SC-13	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise une cryptographie approuvée par le CSTC (https://www.cse-cst.gc.ca/fr/publication/itsa-11e) pour protéger les données classifiées.

Insérer :

AC-11	VERROUILLAGE DE SESSION	(A) Le système d'information empêche tout autre accès au système en verrouillant la session après un délai d'inactivité après un maximum de quatre (4) heures ou à la réception d'une demande d'un utilisateur. (B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur réinitialise l'accès en exécutant les procédures établies d'identification et d'authentification.

Et

AU-9	PROTECTION DE L'INFORMATION DE VÉRIFICATION	(A) Le système d'information protège l'information de vérification et les outils de vérification contre l'accès, la modification et la suppression non autorisés.

Et

IA-5	GESTION DES AUTHENTIFIANTS	Authentification axée sur les mots de passe – Le système d'information : (a) applique un mot de passe de complexité minimale d'une combinaison de lettres majuscules et minuscules, des numéros et des symboles (p. ex., @, #, $, %); (c) chiffre les mots de passe stockés et en transit; (d) applique les restrictions minimales et maximales de durée des mots de passe, soit 180 jours ou moins; et (e) interdit la réutilisation des mots de passe pendant 3 générations.

Et

SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES	L'organisation produit, contrôle et distribue des clés cryptographiques symétriques et asymétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC. L'ARC acceptera les protocoles et les suites de chiffres compatibles qui répondent aux conseils fournis dans les documents ITSB-60 (https://www.cse-cst.gc.ca/fr/node/253/html/15204) et ITSA-11E (https://www.cse-cst.gc.ca/fr/node/227/html/15164) du CSTC. L'organisation a la souplesse d'ajuster la liste des protocoles et des suites de chiffres pris en charge afin de tenir à jour les navigateurs grand public, tout en respectant les normes du CSTC. Par exemple, les navigateurs largement utilisés tels qu'Internet Explorer, Chrome, Firefox, Safari et Opera prennent en charge le protocole TLS 1.0/1.1/1.2, tel qu'il est exigé par le document ITSB-60, et les suites de chiffres qui utilisent l'algorithme SHA-256, tel qu'il est indiqué dans le document ITSA-11E.
SC-13	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise une cryptographie approuvée par le CSTC pour protéger les données classifiées. L'ARC acceptera les protocoles et les suites de chiffres compatibles qui répondent aux conseils fournis dans les documents ITSB-60 (https://www.cse-cst.gc.ca/fr/node/253/html/15204) et ITSA-11E (https://www.cse-cst.gc.ca/fr/node/227/html/15164) du CSTC. L'organisation a la souplesse d'ajuster la liste des protocoles et des suites de chiffres pris en charge afin de tenir à jour les navigateurs grand public, tout en respectant les normes du CSTC. Par exemple, les navigateurs largement utilisés tels qu'Internet Explorer, Chrome, Firefox, Safari et Opera prennent en charge le protocole TLS 1.0/1.1/1.2, tel qu'il est exigé par le document ITSB-60, et les suites de chiffres qui utilisent l'algorithme SHA-256, tel qu'il est indiqué dans le document ITSA-11E.

TOUTES AUTRES MODALITÉS DU CONTRAT DEMEURENT SANS CHANGEMENT.