DEMANDE DE RENSEIGNEMENTS (DDR) RELATIVE AUX

SOLUTIONS EN MATIÈRE DE SÉCURITÉ DES BASES DE DONNÉES

RFI - Database Security_v7_Sept_25_2014_FR.docx

Table des matières

PARTIE A – OBJECTIFS GÉNÉRAUX

A1.0 OBJECTIF DE LA DEMANDE DE RENSEIGNEMENTS (DDR)

L'Agence des services frontaliers du Canada (ASFC) examine différentes options qui fourniront une fonction de sécurité et de vérification pour ses archives de données. La présente DDR vise principalement à obtenir des commentaires des fournisseurs concernant une solution commerciale qui favorise une gestion de la politique en matière de sécurité des données à l'échelle de l'organisation et qui répond aux besoins de l'ASFC. Cela permettra à l'ASFC de se faire une idée des types de solutions commerciales offertes sur le marché ainsi que de leurs capacités.

Nota : La solution proposée et mentionnée dans les réponses aux questions fournies doit être actuellement offerte sur le marché.

PARTIE B – PRÉSENTATION DES RÉPONSES

B1.0 INSTRUCTIONS RELATIVES À LA PRÉPARATION DE LA RÉPONSE

B1.1 L'ASFC demande aux fournisseurs de présenter leurs réponses en sections distinctes, comme suit :

a. Une copie papier et une copie électronique sur CD en format Microsoft Word. L'ASFC demande que les fournisseurs suivent les instructions décrites ci-après pour préparer leur réponse :
   i. utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm);
   ii. utiliser un système de numérotation correspondant à celui de la DDR.

b. Conformément à la Politique d'achats écologiques. En avril 2006, le Canada a émis une politique imposant aux ministères et aux organismes fédéraux de prendre les mesures nécessaires pour intégrer des facteurs environnementaux au processus d'approvisionnement. Voir la Politique d'achats écologiques (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html). Pour aider le Canada à atteindre ses objectifs, les fournisseurs devraient :

   i. utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et contenant au moins 30 % de matières recyclées;

   ii. utiliser un format qui respecte l'environnement, soit une impression en noir et blanc plutôt qu'en couleur, une impression recto verso, des agrafes ou des trombones plutôt qu'une reliure à anneaux plastiques, un classeur à attaches ou une reliure.

B1.2 Les fournisseurs doivent présenter leur réponse au plus tard le : 16 octobre, 2014

B1.3 Les fournisseurs **doivent** transmettre leurs demandes de renseignements et leurs réponses à la présente DDR en utilisant l'adresse de livraison ci-dessous :

Adresse de livraison : Agence des services frontaliers du Canada
Secteur de distribution des chèques et de réception des soumissions
473, rue Albert, 6e étage
Ottawa (Ontario) K1A 0L8
La Réception des soumissions est ouverte du lundi au vendredi inclusivement, de 8 h 30 à 11 h 30, à l'exclusion des jours fériés.

B1.4 L'examen des réponses sera entrepris après la date et l'heure indiquées ci-dessus. Les réponses reçues après cette date pourraient ne pas être examinées.

B1.5 Si la réponse n'est pas suffisamment claire, l'ASFC se réserve le droit de chercher à obtenir des renseignements supplémentaires à son entière discrétion.

B2.0 RESPONSABLES

B2.1 AUTORITÉ CONTRACTANTE

L'autorité contractante est chargée de gérer le processus d'approvisionnement et de DDR.

Aleksandra Green
Agent de négociation des marchés
Direction générale du contrôle
Agence des services frontaliers du Canada
473, rue Albert
Ottawa (Ontario) K1A 0L8
Téléphone : 613-960-3350
Courriel : aleksandra.green@cbsa.gc.ca

B3.0 SÉANCE D'INFORMATION À L'INTENTION DE L'INDUSTRIE

B3.1 SÉANCES DE DÉMONSTRATION INTERACTIVES À L'INTENTION DES FOURNISSEURS

L'ASFC peut, à son entière discrétion, tenir des rencontres avec les fournisseurs intéressés afin de leur donner l'occasion de présenter et de démontrer leurs compétences en ce qui concerne la présente DDR ainsi que d'en discuter.

Les fournisseurs qui ont exprimé leur intérêt peuvent s'attendre à ce que l'on communique avec eux environ dans les deux semaines suivant la date de clôture de la DDR pour fixer la date de la séance à l'intention des fournisseurs. Le programme de la rencontre ainsi qu'une liste des questions précises ou des domaines d'intérêt à traiter au cours de la séance seront remis aux fournisseurs intéressés.

La séance à l'intention des fournisseurs aura lieu dans la région de la capitale nationale. L'emplacement et l'horaire exacts seront indiqués dans l'invitation. Les fournisseurs devront également fournir une version électronique de leur présentation.

La séance à l'intention des fournisseurs portera sur des aspects fonctionnels et techniques particuliers du logiciel commercial de sécurité des bases de données. À cette fin, les représentants des fournisseurs qui prendront part à la séance doivent comprendre des experts en la matière qui pourront répondre adéquatement aux questions qui seront posées. Des membres du personnel de l'ASFC possédant une vaste expérience en technologie de l'information (TI) assisteront à la présentation.

B4.0 Réponses de l'industrie

B4.1 Format de la réponse

Pour faciliter l'utilisation et tirer profit au maximum des réponses, l'Agence demande aux fournisseurs de suivre la structure décrite à l'Annexe A – Exigences relatives aux réponses.
Il n'y a pas de limite imposée quant au nombre de pages de renseignements fournis.

B4.2 Langue de la réponse

Les réponses peuvent être fournies en français et en anglais, au choix du fournisseur.

B4.3 Paramètres de la réponse

On rappelle aux fournisseurs qu'il s'agit ici d'une DDR et non d'une demande de propositions (DP) et que, pour cette raison, ils ne doivent pas hésiter à faire part de leurs commentaires, de leurs préoccupations et, s'il y a lieu, de leurs recommandations quant à la façon dont l'exigence pourrait être satisfaite.

B4.4 Confidentialité de la réponse

Les fournisseurs sont priés d'indiquer clairement les éléments de leur réponse pour lesquels ils détiennent des droits de propriété exclusive. Les réponses de chacun des fournisseurs demeureront confidentielles.

PARTIE C – Stratégie d'approvisionnement

À l'heure actuelle, l'ASFC ne prévoit pas avoir recours à une DP. La présente DDR vise uniquement à recueillir des renseignements, tel qu'il est décrit à la Partie A.

ANNEXE A – EXIGENCES RELATIVES AUX RÉPONSES

La présente DDR vise à obtenir des renseignements détaillés des fournisseurs. L'ASFC a dressé une liste de questions ci-dessous et demande aux fournisseurs de donner des réponses détaillées, afin que l'Agence puisse réunir des renseignements sur les produits de sécurité des données offerts sur le marché.

La présente DDR ne constitue pas un engagement à l'égard d'achats ou de marchés futurs. Nota : La solution proposée et mentionnée dans les réponses aux questions fournies doit être actuellement offerte sur le marché. Au moment de rédiger leurs réponses, les fournisseurs doivent se reporter à l'Appendice A – Renseignements sur l'environnement technique de l'ASFC.

L'ASFC demande aux fournisseurs de fournir ce qui suit :

1. PROFIL DE L'ENTREPRISE

Chaque fournisseur doit fournir les renseignements suivants :

a. Le nom, l'adresse, le numéro de téléphone, le numéro de télécopieur et les adresses électroniques de l'entreprise.
b. Le nom de la personne ressource de l'entreprise et son numéro de téléphone.
c. Des renseignements généraux sur l'entreprise (emplacement de la société mère; coordonnées du représentant de l'entreprise et du distributeur au Canada, le cas échéant; type de produits vendus et adresse du site Web). L'ASFC peut demander des coordonnées supplémentaires en tout temps.

2. DESCRIPTION DE LA SOLUTION

Chaque fournisseur doit fournir les renseignements suivants :

a. Un identificateur de la solution, comme un numéro de modèle, un numéro de version et une description de tous les éléments nécessaires à la solution.
b. Des dépliants décrivant les caractéristiques de l'équipement et fournissant des renseignements détaillés sur l'équipement doivent être compris dans les réponses à la présente lettre d'intérêt.
c. Un modèle de calcul des coûts.
d. Un modèle d'octroi de licences.
e. Les niveaux de service en matière de soutien et d'entretien.

3. QUESTIONS

L'ASFC demande aux fournisseurs de répondre aux questions ci-dessous.

TABLEAU 1 – QUESTIONS LIÉES À L'ARCHITECTURE

Question de l'ASFC	Réponse du fournisseur
1. Comment la solution peut-elle être intégrée aux fonctions et comment fournira-t-elle l'ensemble de ses fonctions, notamment la capacité de l'ASFC de surveiller, de contrôler et de vérifier l'accès à ses données, à l'environnement en entier? (Consultez l'Appendice A – Renseignements sur l'environnement technique de l'ASFC pour obtenir des renseignements sur l'environnement en entier.)	
2. Comment la solution permet-elle à l'ASFC de protéger ses données d'applications Web internes et externes et comment répond-elle aux besoins en matière d'intégration particuliers requis pour avoir accès à l'ensemble des fonctions de la solution? (Consultez l'Appendice A – Renseignements sur l'environnement technique de l'ASFC pour obtenir des renseignements sur les besoins en matière d'intégration particuliers requis.)	
3. Comment la solution fournit-elle l'ensemble de ses fonctions sans causer une charge supplémentaire relativement à l'utilisation de l'unité centrale de traitement (UCT) et à la consommation de la mémoire vive pour les bases de données existantes, les nouvelles bases de données et les serveurs d'applications?	

TABLEAU 2 – QUESTIONS LIÉES AUX FONCTIONS

Question de l'ASFC	Réponse du fournisseur
4. Comment la solution gère-t-elle les difficultés liées à la sécurité des données et des bases de données ci-dessous? a. Accès des utilisateurs et contrôle de l'accès. Comment la solution isole-t-elle	

Question de l'ASFC	Réponse du fournisseur
ou contrôle-t-elle l'accès des utilisateurs aux données? b. Registres de vérification. La solution produit-elle des enregistrements de vérification qui contiennent, au minimum, des données sur les actions effectuées par l'entremise des comptes d'utilisateur, de service et du système? i. Type (p. ex. ouverture et fermeture de session, changement de configuration). ii. Moment (p. ex. 2013-01-01, 5 h, HNE). iii. Endroit (p. ex. ID du système). iv. Source (p. ex. ID du poste de travail). v. Résultat (p. ex. réussite, échec). vi. Identité (p. ex. ID du compte d'utilisateur, ID du compte de service, ID du compte du système). c. La solution vérifie-t-elle les accès effectués par l'entremise de comptes assortis de droits d'accès privilégiés, comme un compte d'administrateur ou d'administrateur de système? d. La solution avise-t-elle les administrateurs et effectue-t-elle des mesures de récupération configurées si le service de vérification de la solution échoue ou est désactivé par inadvertance? Le cas échéant, décrire comment. e. Le service de traitement des exceptions de la solution consigne-t-il toutes les exceptions et les défaillances dans un registre d'anomalies? f. Comment les utilisateurs autorisés accèdent-ils aux registres de vérification, et comment ces derniers sont-ils protégés contre l'accès, la modification et la suppression non autorisés? g. La solution produit-elle des rapports dans un format lisible pour les enregistrements	

Question de l'ASFC	Réponse du fournisseur
de vérification? h. La solution permet-elle d'envoyer des enregistrements de vérification à un dépôt central? i. La solution permet-elle de chiffrer les noms d'utilisateur et les mots de passe pour passer de l'appareil du client aux serveurs? j. La solution génère-t-elle des marques d'horodatage pour les enregistrements de vérification? Le cas échéant, la solution utilise-t-elle des horloges de système internes, et contiennent-elles la date et l'heure (à la seconde près)? Dans l'affirmative, l'heure est-elle affichée selon le temps universel coordonné (UTC) ou selon l'heure locale décalée par rapport à l'UTC? Le cas échéant, l'horloge de la solution peut-elle être synchronisée avec une source de temps faisant autorité définie par le client? k. Où les enregistrements de vérification sont-ils stockés dans la solution? Cet endroit peut-il être adapté? l. La solution permet-elle de configurer la période de rétention d'un registre de vérification? m. La solution vérifie-t-elle les accès en mode lecture des données effectués par les utilisateurs et les administrateurs?	
5. Comment la solution permet-elle de gérer les mots de passe et les privilèges par défaut des comptes d'utilisateur, de service et du système?	
6. La solution peut-elle être renforcée, ce qui comprend la capacité de désactiver ou de supprimer des éléments et des services inutiles ainsi que des noms d'utilisateurs et des mots de passe? Dans l'affirmative, veuillez décrire comment.	

Question de l'ASFC	Réponse du fournisseur
7. Comment la solution permet-elle de surveiller de façon continue les données de nature délicate? Comment émet-elle des alertes en temps réel en cas d'infraction grave? Comment les définit-elle et comment les repère-t-elle?	
8. Votre organisation a-t-elle établi un processus qui indique les correctifs de sécurité liés à la solution? Le cas échéant, comment ces correctifs de sécurité sont-ils offerts?	
9. Votre organisation a-t-elle établi un processus qui cerne les vulnérabilités de la solution? Dans l'affirmative, comment les mesures requises pour corriger ces vulnérabilités sont-elles offertes?	
10. Fournissez-vous des documents à l'intention de l'administrateur et de l'utilisateur, notamment les guides de renforcement applicables, pour la solution? Le cas échéant, veuillez décrire les sujets sur lesquels ils portent.	

TABLEAU 3 – QUESTIONS LIÉES À L'INTÉGRATION

Question de l'ASFC	Réponse du fournisseur
11. La solution peut-elle être intégrée aux services et aux protocoles d'identification, d'authentification et d'autorisation d'IBM z/OS (p. ex. fonction de contrôle de l'accès et fonction de contrôle de l'accès aux données)? Le cas échéant, veuillez décrire comment.	
12. La solution peut-elle être intégrée aux services et aux protocoles d'identification, d'authentification et d'autorisation d'Active Directory de Microsoft Windows (p. ex. Protocole allégé d'accès annuaire; Kerberos)? Le cas échéant, veuillez décrire comment.	
13. La solution peut-elle être intégrée aux objets Stratégie de groupe de Microsoft Windows? Le cas échéant, veuillez décrire comment.	
14. La solution peut-elle être intégrée à Tivoli Endpoint Manager et à Software Update Service de Microsoft Windows? Le cas échéant, veuillez décrire comment.	

Question de l'ASFC	Réponse du fournisseur
15. La solution peut-elle être intégrée à Host Intrusion Prevention de McAfee, à Policy Auditor de McAfee et à VirusScan Enterprise de McAfee avec Anti-Spyware géré par ePolicy Orchestrator de McAfee? Le cas échéant, veuillez décrire comment.	
16. La solution permettrait-elle de communiquer de façon sécuritaire les avis d'événements critiques, et cela peut-il être adapté? Le cas échéant, veuillez décrire comment.	
17. La solution permet-elle d'assurer la gestion au moyen de connexions sécurisées qui utilisent le protocole IPSec AES-256, le protocole TLS v1.1 ou supérieure avec le protocole SSL v3.0 ou supérieure ou le protocole SSH v2.0 ou supérieure? Le cas échéant, veuillez décrire comment.	
18. La solution doit-elle être branchée ou liée à votre infrastructure de réseau?	

TABLEAU 4 – QUESTIONS LIÉES AU SOUTIEN

Question de l'ASFC	Réponse du fournisseur
19. Comment fournissez-vous un soutien pour la solution, notamment l'application des correctifs de sécurité, la mise en œuvre des mesures de correction des vulnérabilités connues et le dépannage et la résolution d'incidents ou de problèmes liés aux modules cryptographiques (s'il y a lieu)?	

TABLEAU 5 – QUESTIONS LIÉES AUX NORMES

Question de l'ASFC	Réponse du fournisseur
20. Les modules cryptographiques (s'il y a lieu) fournis par la solution ont-ils été validés et certifiés par le Programme de validation des modules cryptographiques (PVMC) au moins à la norme Federal Information Processing Standard (FIPS) 140-2?	
21. La solution peut-elle respecter les normes liées à l'infrastructure à clés publiques du gouvernement du Canada, comme celles liées aux identités numériques d'Entrust et à Microsoft?	

TABLEAU 6 – QUESTIONS LIÉES AUX LICENCES

Question de l'ASFC	Réponse du fournisseur
22. Comment accordez-vous habituellement des licences d'utilisation de votre logiciel commercial (c.-à-d. types d'utilisateurs, par serveur, par UCT, utilisateurs simultanés et à l'échelle de l'organisation)?	
23. Combien de licences d'utilisation individuelles faut-il acheter pour obtenir une licence d'utilisation à l'échelle de l'organisation?	

4. AUTRES SUGGESTIONS

Avez-vous (le fournisseur) des suggestions ou des préoccupations à l'égard des tâches et des questions énumérées à l'Annexe A? Dans l'affirmative, veuillez les énoncer et formuler toute recommandation que vous pourriez appliquer pour y répondre.

5. DÉMONSTRATIONS

Seriez-vous intéressé à assister à une séance de suivi de la DDR dans le but de faire une démonstration de votre logiciel commercial? La séance peut avoir lieu sur place à un bureau de l'ASFC ou à distance par l'entremise d'une conférence Web ou d'une vidéoconférence. Consultez la partie Séances de démonstration interactives pour obtenir de plus amples renseignements.

APPENDICES

APPENDICE A – RENSEIGNEMENTS SUR L'ENVIRONNEMENT TECHNIQUE DE L'ASFC

Contexte

L'Agence du revenu du Canada (ARC) et Services partagés Canada (SPC) fournissent des services d'infrastructure à l'Agence des services frontaliers du Canada (ASFC).

Environnement Windows « géré »

L'environnement informatique réparti (EIR) est une infrastructure client-serveur constituée de serveurs, d'ordinateurs de bureau et d'ordinateurs portables Windows, dont les services d'annuaire dorsaux sont assurés par Active Directory (AD). Des centaines de sites au Canada sont pris en charge par l'EIR. La taille de ces sites varie de deux utilisateurs à des centaines d'utilisateurs dans un seul immeuble. La bande passante qu'ils utilisent varie également. Généralement, un site réparti comprend un serveur de fichiers et d'impression et peut-être un serveur Exchange. Les services Exchange seront entièrement centralisés d'ici 2015. La centralisation des services de fichiers et d'impression locaux est à l'étude. Les contrôleurs de domaine AD locaux ou centralisés s'occupent des services d'annuaire de l'environnement géré.

L'ASFC exploite également la plateforme de services de terminal (TSP) à l'aide de Citrix. Cette plateforme est constituée de serveurs centraux, situés dans la région de la capitale nationale, qui hébergent divers services et applications pour un groupe donné d'utilisateurs. Ces services et applications comprennent des applications opérationnelles et des applications bureautiques comme, entre autres, MS Office, Outlook et Exchange ainsi qu'un logiciel d'émulation d'ordinateur central (Attachmate) et des services de fichiers et d'impression de base. De plus, l'ASFC utilise le logiciel de virtualisation d'applications Softgrid pour améliorer l'accès à l'application et la gestion sur l'ensemble de la plateforme TSP.

Voici la liste des principaux logiciels Windows installés dans l'EIR de l'ASFC :

- MS Windows Server 2008
- XenApp (Citrix)
- Windows 7 Enterprise SP1 32 bits (avec BitLocker)
- MS Office 2010
- MS Exchange 2010
- Entrust Security Provider 9.2 et Entrust Security Provider 9.1 pour Outlook
- VirusScan Enterprise v8.8 de McAfee avec Anti-Spyware, Host Intrusion Prevention v8.0, Policy Auditor 6.0 géré par les services ePO de McAfee
- Tivoli Endpoint Manager pour le déploiement de logiciels, l'inventaire et le contrôle à distance.
- WSUS de Microsoft pour les mises à jour de correctifs de plateforme

La version de Java Runtime Environment (environnement d'exécution Java [JRE]) installée sur tous les ordinateurs de bureau a été mise à niveau de 1.6.0_18 vers 1.7.

Le matériel sous-jacent pour l'environnement Windows est constitué de serveurs basés sur les architectures AMD et Intel qui utilisent la technologie multicœur et multiprocesseur. Les ordinateurs de bureau et les ordinateurs portables sont également basés sur les architectures AMD et Intel; ils utilisent des processeurs multicœurs et une mémoire à double canal.

La plateforme est considérée comme « gérée », car tous les postes de travail respectent les normes concernant les outils de sécurité standard et les correctifs mensuels de système d'exploitation. En outre, tous les appareils sont créés en tant qu'objets dans AD et sont assujettis aux politiques obligatoires relatives à la sécurité des appareils. Des politiques comme celles visant l'exécution des scripts, l'administration locale et l'accès en fonction des rôles sont attribuées à chaque appareil enregistré dans le domaine. Ces politiques peuvent être personnalisées pour respecter de nombreuses exigences de l'ASFC s'appliquant à des appareils précis. Il est également possible de personnaliser automatiquement le déploiement des logiciels essentiels et obligatoires grâce aux produits Tivoli.

Environnement des bases de données

Les archives de données de l'ASFC reposent sur la configuration SYSPLEX de l'ordinateur central z/OS et sur l'environnement Linux, Unix et Windows (LUW) entre deux centres de données pour des raisons de reprise.

Stockage des données :

- DB2 pour z/OS;
- DB2 dans un environnement LUW;
- DB2 (MPP) dans un environnement LUW;
- Serveur SQL;
- Sybase;
- Postgres;
- PureData Database Appliance;
- Données non enregistrées dans des bases de données (VSAM, PDF, fichier non hiérarchique, etc.).

Les applications reposent sur une architecture client-serveur à deux et à trois niveaux.