

Return Bids to: - Retourner les soumissions à :

Shared Services Canada / Services partagés Canada

C/O Andrew Nimmo (Contracting Authority)

Andrew.nimmo@canada.ca

**180 Kent St., 13th Floor,
Ottawa, ON, K1G 4A8**

**REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION**

Proposal To: Shared Services Canada

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 or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out thereof.

Proposition aux: Services partagés Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexées, au(x) prix indiqué(s)

Title – Sujet Solution de gestion des vulnérabilités d'entreprise	
Solicitation No. – N° de l'invitation 15-010876/A	Amendment No. – N° de modif. 007
Client Reference No. – N° référence du client 15-010876/A	Date 2017-01-26
File No. – N° de dossier 019eo-15-33922/A	
Solicitation Closes – L'invitation prend fin at – à 02 :00 PM on – le 2017-02-13	Time Zone Fuseau horaire Heure normale de l'Est HNE
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input checked="" type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Inquiries to : - Adresser toutes questions à: Nimmo, Andrew	Buyer Id – Id de l'acheteur 019eo
Telephone No. – N° de téléphone : 819-956-0728	FAX No. – N° de FAX Not applicable
Delivery required - Livraison exigée See Herein	Delivered Offered – Livraison proposée
Destination – of Goods, Services, and Construction: Destination – des biens, services et construction : See Herein	

Solicitation No. - N° de l'invitation
15-010876/A

Amd. No. - N° de la modif.
007

Buyer ID - Id de l'acheteur

Client Ref. No. - N° de réf. du client

File No. - N° du dossier

CCC No./N° CCC - FMS No/ N° VME

Vendor/firm Name and address

Raison sociale et adresse du fournisseur/de l'entrepreneur

Facsimile No. – N° de télécopieur

Telephone No. – N° de téléphone

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

MODIFICATION 007

Cet amendement est porté à:

- 1) Répondre aux questions des soumissionnaires concernant le contenu de la DP, tel qu'énoncé dans Appendice 001;
 - 2) Modifier la demande de proposition (DP), comme indiqué à l'annexe 002;
-

Appendice 001

Question 37

Pour la question 20:

Veillez indiquer le nombre de périphériques d'éléments de réseau (physiques et virtuels) utilisant une adresse IP unique tels que les routeurs, les commutateurs, le pare-feu, les équilibreurs de charge, etc. Autrement dit - Sur les 300 000 appareils, combien sont les imprimantes et combien sont des réseaux Comme décrit ci-dessus.

Réponse 37

a Couronne estime l'inventaire actuel des dispositifs d'éléments de réseau à 247 000 appareils. La Couronne estime l'inventaire actuel des imprimantes réseau à 53 000 appareils

Question 38

Référence Obligation M6 et amendement 001 du Canada, réponse 001: Dans sa réponse à la question 1, le Canada a confirmé qu'il n'existait pas aujourd'hui de solution de balayage de vulnérabilité incantée active dans l'environnement du SSC, mais «de nombreux environnements patrimoniaux» et solutions). De plus, le Canada demande que la solution des soumissionnaires doit cohabiter avec ces solutions multiples au cours d'une période de transition qui reste à définir pour obtenir une solution centralisée.

Actuellement, il existe plus de 50 outils de balayage de vulnérabilité commerciaux et open source disponibles sur le marché, et environ 35 entreprises proposent des solutions pour OWASP (Open Web Application Security Project). Malheureusement, il n'existe pas de format standardisé parmi ces solutions de fournisseur qui limite aujourd'hui l'importation ou l'échange de données de vulnérabilité entre les solutions avec la plupart des fournisseurs de développer leurs solutions en utilisant leur propre mise en forme propriétaire et les brevets individuels.

Nous comprenons le désir du Canada de faire en sorte que l'offre de Bidder satisfasse aux exigences obligatoires de la SSC énoncées dans M6 et que l'avantage qu'elle pourrait apporter à cette transition soit trop restrictif pour tous les fournisseurs de scanners de vulnérabilité et trop incertain puisque le Canada n'a fourni aucun détail Concernant l'environnement actuel.

À la lumière de ces défis qui sont susceptibles de faire face à la volonté de tous les soumissionnaires SSC:

- A) l'amendement M6 est-il obligatoire et obligatoire pour une exigence cotée?
- B) Fournir le calendrier de mise en œuvre proposé par SSC de la «cohabitation» à une solution centralisée?
- C) Fournir une liste de solutions actives dans l'environnement aujourd'hui que SSC aimerait maintenir pendant la période de mise en œuvre et de transition?

Réponse 38

A) Veuillez consulter les formulaires 3 et 4 révisés le 20 janvier 2017.xls affichés sur la page Web de la DP.

<https://buyandsell.gc.ca/procurement-data/tender-notice/PW-17-00762407>

B) La Couronne n'a pas accepté de reformuler la DP pour y inclure la «cohabitation». Le courant, en place

Les solutions de vulnérabilité ont des licences expirant dans environ 1 an. Les solutions de vulnérabilité en place seront migrées vers la solution Enterprise lors du renouvellement.

C) Veuillez consulter les formulaires 3 et 4 révisés le 20 janvier 2017.xls affichés sur la page Web de la DP.

<https://buyandsell.gc.ca/procurement-data/tender-notice/PW-17-00762407>

Question 39

M2 déclare "Une analyse de 10 000 adresses IP non basée sur les certificats doit être effectuée sur une période de 2 jours, échelonnée sur les heures de non-production pour avoir un impact limité sur les opérations quotidiennes".

Est-ce que la signification de «scannage complet non basé sur des informations d'identification» signifie la numérisation de tous les 65 535 ports TCP et UDP? Étant donné que la communication UDP est sans connexion, les analyses de ports UDP peuvent prendre beaucoup plus de temps que les numérisations de port TCP.

Quelles sont les heures de non-production par jour?

Les heures de non-production varient-elles du jour de la semaine au week-end?

Réponse 39

En raison des différents fuseaux horaires à travers le Canada, la Couronne considère les heures de non-production comme 20:00 à 06:00 heure de l'Est, 7 jours par semaine.

Question 40

M16 indique "La solution doit imposer une relation de confiance / authentifiée avec la source des informations de vulnérabilité."

Est-ce demander où le logiciel reçoit-il feed de vulnérabilité?

Habituellement, chaque fournisseur de logiciel de gestion des vulnérabilités gère les informations de vulnérabilité. Cette exigence demande-t-elle le déroulement du processus, par exemple comment chaque entreprise vérifie que les informations de vulnérabilité sont correctes?

Réponse 40

Clarification: M16 se rapporte aux canaux de communiqués de confiance entre la Couronne et le vendeur pour les mises à jour logicielles de la solution.

Question 41

M17 déclare: «La solution doit pouvoir interagir avec les informations de vulnérabilité de la base de données nationale de vulnérabilité (NVD) pour les sources d'alimentation de données.

Quel type d'interface est attendue? Est-ce simplement une référence à la NVD suffisante pour chaque vulnérabilité, ou y a-t-il une interface supplémentaire requise?

Réponse 41

La Couronne s'attend à ce qu'un lien et des détails de référence renvoient à la NVD ou à la source déclarée de l'information sur la vulnérabilité à l'égard de chaque vulnérabilité.

Question 42

M20 - La solution doit permettre de s'assurer que tous les journaux / informations de débogage / vidages de mémoire peuvent être désinfectés pour des informations sensibles afin qu'ils puissent être partagés pour le support des fournisseurs.

Pourriez-vous clarifier ce qui est considéré comme de l'information sensible? Numéros de carte de crédit, adresses IP, noms d'utilisateur, mots de passe, etc?

Réponse 42

La Couronne considère toutes les données pouvant identifier la Couronne, les biens de la Couronne ou les employés de la Couronne comme étant sensibles aux données. Les informations d'identification utilisateur, le nom, le nom et le prénom d'un utilisateur, les mots de passe, les adresses IP, le nom du serveur, le nom de l'utilisateur final, l'emplacement et la carte de crédit.

Question 43

M22 indique "La solution doit être capable d'effectuer une analyse de la conformité de la configuration sans agent et sans agent."

Combien d'agents sont attendus?

Réponse 43

À l'heure actuelle, la Couronne ne peut pas estimer le nombre d'agents qui sont attendus. La Couronne suppose que le nombre d'agents variera en fonction des solutions proposées par les diverses solutions de fournisseurs sur la DP. La Couronne s'attend à ce que les fournisseurs fournissent les détails quant au nombre d'agents qu'ils seront en attente.

Question 44

Pour le réseau SSC inclus dans cette DP, sera-t-il un réseau autonome ou y aura-t-il des ministères partenaires externes sur d'autres réseaux / qui seront soutenus également dans ce cadre?

Réponse 44

La solution Entreprise sera élargie pour inclure les départements partenaires externes sur d'autres / leurs propres réseaux.

Question 45

La colonne L et J du premier onglet de la feuille de tarification ne reflète pas les bonnes formules. La Couronne peut-elle amender et renvoyer?

Réponse 45

Veillez vous référer à l'annexe 002 de cet amendement

Question 46

SOW 7.2.2 est requis dans le contrat initial (1er onglet) et optionnel (2e onglet). En réponse à Q30, il est dit: «La Couronne ne prévoit pas la croissance des stocks jusqu'à 2 000 000 jusqu'à la fin du contrat de 5 ans.

je. Veuillez préciser pourquoi la croissance au-delà des 2 millions d'appareils initiaux (c.-à-d. SOW 7.2.2) devrait être comptabilisée dans le contrat initial (1er onglet)

Réponse 46

La Couronne exige l'option d'acheter des licences supplémentaires et / ou de la capacité matérielle au prix d'enchère initial fixé dans le contrat si nos exigences dépassent les 2 000 000 exigences de l'appareil. Option d'achat d'une année supplémentaire de soutien pour un maximum de trois (3) ans au prix d'enchère original. Option d'achat d'un ou plusieurs forfaits de formation de cinq (5) jours pour un maximum de trois (3) ans au prix fixé par enchère.

Question 47

Réponse à Q21 états "Actuellement, les estimations de la Couronne ont 100 000 serveurs et 600 000 appareils de bureau. Un déploiement complet de la solution et l'échelle jusqu'à 2000000 dispositifs seraient échelonnés sur plusieurs années. "

ii) . La Couronne peut-elle prévoir une croissance estimée entre la première et la cinquième année, car cela pourrait avoir une incidence sur notre modèle de tarification?

Réponse 47

La Couronne exige 500 000 initialement jusqu'à 2 000 000 dans le cadre du contrat, la Couronne prévoit une croissance estimée de 20% par an sur le contrat de 5 ans, la croissance sera couverte par les 3 années option dans les tables de tarification.

Question 48

La table de tarification ne prend pas en compte les besoins en matériels et logiciels de laboratoire (SOW 7.3.1). La Couronne peut-elle préciser où nous devrions tenir compte de ce coût dans les finances?

Réponse 48

Veillez vous référer à l'annexe 002 de cet amendement

Question 49

Lors de l'attribution du contrat, quelle est la stratégie de remplacement de la Couronne en ce qui a trait à la suppression d'autres scanners de fournisseurs et à la normalisation avec le fournisseur sélectionné? Veuillez fournir des estimations annuelles.

Réponse 49

À l'heure actuelle, la SSC compte environ 185 scanners d'évaluation de la vulnérabilité prenant en charge plusieurs numéros d'adresses IP par licence. Les renouvellements de soutien sont effectués annuellement et seront répartis sur le contrat de 5 ans. Il n'est pas possible de fournir des estimations de numérisation annuelle parce que les départements partenaires disposent de plusieurs numéros de scanners et dépendra de l'année où le partenaire a été embarqué dans la solution d'entreprise.

Question 50

En ce qui concerne Common Criteria, EAL3 / EAL3 + impose au fournisseur des exigences supplémentaires pour la documentation des pratiques et des procédures liées à la gestion de la configuration, à la sécurité de l'environnement de développement et au modèle de cycle de vie du développeur, mais ne prescrit aucun mécanisme allant au- . EAL2 / EAL2 + et EAL3 / EAL3 + partagent le même niveau d'analyse de vulnérabilité, de tests de pénétration et de tests indépendants. Ainsi, une évaluation EAL3 / EAL3 + ne représente pas une augmentation significative de l'assurance de sécurité fournie par une évaluation EAL2 / EAL2 +.

B. Nous demandons donc à la Couronne de modifier la R23,

"La solution doit avoir la certification Critères communs à EAL2 + ou EAL3 ou supérieur pour s'assurer que le produit a été testé et examiné de manière adéquate."

Réponse 50

La Couronne avait déjà fait passer cette exigence d'une obligation obligatoire à une obligation cotée. Le Centre canadien de la sécurité a déclaré que la solution exige une cote EAL3, de sorte que la Couronne ne réduira pas davantage cette exigence.

Question 51

R1: La solution devrait prendre en charge les serveurs centralisés de gestion et de reporting qui peuvent fonctionner indépendamment (y compris leurs scanners et agents dépendants respectifs), et être subordonné à un échelon supérieur de serveurs de gestion et de reporting. Les serveurs de gestion et de génération de rapports doivent prendre en charge plusieurs niveaux hiérarchiques de serveurs de gestion et de rapport subordonnés (y compris leurs scanners et agents dépendants respectifs).

une. Pouvez-vous fournir plus de détails sur les exigences pour la gestion centralisée et les serveurs de rapports fonctionnant indépendamment? Qu'est-ce que l'indépendance implique?

B. Combien de niveaux de serveurs de gestion et de reporting subordonnés le SSC prévoit-il pour les hiérarchies des exigences?

C. Combien de hiérarchies différentes de serveurs centralisés de gestion et de reporting sont prévues?

Réponse 51

A) L'indépendance impliquerait la possibilité de déployer une solution auprès d'un partenaire externe, ce qui permettrait au partenaire d'effectuer toutes les fonctions nécessaires, mais de rassembler toutes les informations dans une solution de SSC.

B) La Couronne ne peut donner de réponse parce qu'elle peut varier selon la solution. Cet effort sera déterminé dans le cadre des travaux décrits dans la SOW.

C) La couronne ne peut donner de réponse parce qu'elle peut varier selon la solution. Cet effort sera déterminé dans le cadre des travaux décrits dans la SOW.

Question 52

M4 La solution doit être capable de personnaliser la hiérarchisation des risques en fonction du contexte commercial.

Question. La Couronne peut-elle préciser et préciser le sens du contexte commercial en ce qui Solution VMS

Réponse 52

La couronne requiert la capacité d'ajuster le score de risque afin d'accroître la hiérarchisation des risques sur les dispositifs critiques. La Couronne déterminerait quels dispositifs sont essentiels à la mission ou nécessaires aux opérations principales en fonction du contexte fonctionnel / opérationnel de l'appareil.

Question 53

En ce qui concerne la R6, le gouvernement du Canada peut-il fournir plus de détails sur les exigences relatives aux «protocoles d'authentification pour la collecte de fichiers» lors de l'intégration avec les technologies SIEM.

Cette exigence demande-t-elle s'il ya des fichiers contenant des journaux d'authentification qui peuvent être ingérés par un SIEM, ou est-ce demander autre chose

Réponse 53

Les protocoles d'authentification énumérés dans l'exigence seront utilisés pour intégrer la solution avec la solution SIEM en place de SSC

Question 54

Cette exigence ne comprend pas plusieurs mécanismes communs pour l'intégration de composants tiers tels qu'une API REST, XML, ODBC / JDBC et SOAP. Veuillez considérer l'ajout de ces mécanismes d'intégration couramment utilisés aux exigences cotées afin de refléter la valeur de ces interfaces basées sur des normes pour la Couronne.

Réponse 54

La Couronne a inclus les mécanismes nécessaires pour interagir avec les technologies SIEM (s) actuellement en place. Les soumissionnaires peuvent énumérer d'autres technologies, mais la Couronne ne changera pas la notation ou le contenu de l'exigence notée 6.

Question 55

Veuillez confirmer que la Couronne acceptera les captures d'écran pour corroborer la fonctionnalité du produit.

Réponse 55

3.2 Section I: Offre technique de la DP indique que le soumissionnaire a la responsabilité de fournir les renseignements nécessaires pour démontrer sa compréhension et sa justification aux exigences. Il appartient aux soumissionnaires de déterminer la meilleure façon de le faire. La solution recommandée sera également assujettie au plan d'essai VCMS avant l'attribution du contrat. Ce plan d'essai sera utilisé pour vérifier un sous-ensemble des exigences obligatoires de la solution VCMS. Seule l'offre gagnante sera soumise à ce plan d'essai; Si le soumissionnaire omet de démontrer les exigences à la satisfaction de SSC, le soumissionnaire sera automatiquement disqualifié et la prochaine enchère admissible sera évaluée.

Question 56

Référence Annexe B Tables de tarification, onglet Articles d'achat et services, postes 1 et 2, 2 ans de soutien contractuel initial.

La SSC peut-elle expliquer pourquoi l'élément de ligne 1 / colonne F n'inclut pas de formule, où l'élément de ligne 2 / colonne F comprend la formule = E10 * F10?

Réponse 56

Veuillez vous référer à l'annexe 002 de cet amendement

Question 57

Référence Annexe B Tables de tarification, onglet Éléments d'achat et services. Notre solution en réponse à la ligne 1 et à la ligne 2 exigera plusieurs numéros de pièce avec des quantités différentes.

Les soumissionnaires sont-ils obligés d'inclure plusieurs codes de produits dans la colonne C?

Réponse 57

Oui, les soumissionnaires peuvent inclure plusieurs numéros de pièces, mais comme il s'agit d'une solution, la quantité doit refléter la quantité requise pour fournir la solution de l'exigence initiale

Question 58

Dans la ligne 2 des tableaux de prix de l'Annexe B, SSC stipule que «PÉRIODE DE CONTRAT INITIALE La période initiale du contrat (HW & SW) comprend deux (2) ans d'entretien et de soutien pour HW et SW». Si elle doit être incluse, pourquoi le SSC a-t-il séparé le prix pour le «prix ferme du lot» de «2 ans de soutien contractuel initial» dans les colonnes E & F? Ou ces deux exigences distinctes?

Réponse 58

Il s'agit de la même exigence, le coût de support et le coût de solution sont traités différemment en interne (capital vs dépenses) lors de l'approvisionnement de telle sorte qu'ils sont éclatés, le soutien de 2 ans dans la colonne F est le soutien requis pour la solution détaillée dans la colonne E.

Question 59

Dans les tableaux de prix de l'annexe B, colonne D, la quantité indiquée est pré-réglée à 1 (un). SSC autorise-t-elle les soumissionnaires à représenter correctement la quantité de codes de produits supérieure à 1 (une) quantité nécessaire pour satisfaire aux exigences minimales de la SOW 7.2, 7.7.2. Et 5.1.2.

Réponse 59

Oui, les soumissionnaires peuvent inclure plusieurs codes de produits supérieurs à 1 (un), mais comme il s'agit d'une solution, la quantité doit refléter la quantité requise pour fournir la solution de l'exigence initiale.

Question 60

Services partagés Canada a publié la Demande de propositions pour une solution de gestion de la vulnérabilité de l'entreprise avec une date de soumission demandée fixée au 6 février 2017, afin d'avoir à fournir à Services partagés une réponse pleinement conforme, nous demandons respectueusement une prolongation de trois semaines La date d'échéance prévue du 6 février 2017

Réponse 60

La Couronne a déjà accordé une prolongation d'une semaine. Le ministère public peut accepter une autre prolongation d'une (1) semaine, jusqu'au 13 février. Veuillez vous référer à l'annexe 002

Appendice 002

MODIFICATION DE LA DEMANDE DE PROPOSITION (DP)

1.0 Modifier la demande de proposition Date de clôture:

À partir du: 6 février 2017

Pour: 13 février 2017

2.0 À LA PARTIE 7 - CLAUSES CONTRACTUELLES RÉSULTANTES, Article 7.20

EFFACER 7.20 Exigences de sécurité

INSERER 7.20 Exigences de sécurité

L'entrepreneur doit, en tout temps pendant l'exécution du contrat, être titulaire d'un examen d'organisation désigné valide (DOS) délivré par la Direction de la sécurité industrielle canadienne (DSIC), Services publics et Approvisionnement Canada (PSPC).

L'entrepreneur et / ou ses employés doivent maintenir un contrôle de sécurité valide au niveau de SECRET, accordé par le Canada et approuvé par Services partagés Canada.

L'entrepreneur et / ou ses employés NE DOIVENT PAS enlever des informations ou des actifs PROTÉGÉS ou CLASSIFIÉS du (des) site (s) de travail identifié (s).

L'entrepreneur et / ou ses employés NE DOIVENT PAS utiliser ses systèmes informatiques pour traiter, produire ou stocker électroniquement des informations ou des données PROTÉGÉES et / ou CLASSIFIÉES.

Les sous-contrats qui contiennent des exigences de sécurité ne doivent PAS être accordés sans la permission écrite préalable de Services partagés Canada.

L'entrepreneur et ses employés doivent se conformer aux dispositions suivantes:

- a) Justice Canada - Loi sur la sécurité de l'information (dernière édition);
- B) Manuel de sécurité industrielle (dernière édition)

3.0 PARTIE 4 - PROCÉDURES D'ÉVALUATION ET BASE DE SÉLECTION, 4.2 Conduite de l'évaluation par étapes

EFFACER B) Étape 2 - Évaluation des besoins assignés:

INSERER B) Étape 2 - Évaluation des besoins assignés:

Les soumissions qui répondent à tous les critères obligatoires seront alors notées en attribuant une note aux exigences notées, qui sont indiquées dans la demande de soumissions par le mot «noté» ou par référence à une note. Les soumissionnaires qui ne soumettent pas les soumissions complètes avec toutes

les informations demandées par la présente demande de soumissions seront notés en conséquence. Les exigences nominales sont décrites dans le formulaire de l'annexe C.

Les soumissionnaires doivent obtenir un pointage minimal de 121,5 / 162 sur les exigences nominales pour être considérés comme sensibles (c'est-à-dire 75% ou plus sur le total des points maximum ponctuels). Dans tous les calculs, le Total Technical Score (TTS) sera arrondi à deux décimales. Les offres qui ne marqueront pas au moins 121,5 / 162 seront déclarées non réactives et seront disqualifiées.

- | | | |
|------------|----------------|---|
| 4.0 | EFFACER | Formulaires 3 et 4 Révisé le 20 janvier 2017 |
| | INSERER | Formulaires 3 et 4 Révisé le 26 janvier 2017 |
| 5.0 | EFFACER | ANNEXE A SOW |
| | INSERER | ANNEXE A SOW Révisé le 26 janvier 2017 |
| 6.0 | EFFACER | ANNEXE B Tableaux de tarification révisés le 13 janvier 2017 |
| | INSERER | ANNEXE B Tableaux de tarification révisés le 26 janvier 2017 |
| 7.0 | EFFACER | Annexe E Liste de contrôle des exigences de sécurité |
| | INSERER | Annexe E Liste de contrôle des exigences de sécurité Révisée le 26 janvier 2017 |