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 0A1/Noyau 0A1
11 Laurier St./11, rue, Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 956-3370

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Service de sécurité géré (SSGGC)	
Solicitation No. - N° de l'invitation 2B0KB-123147/A	**Date** 2012-07-31
Client Reference No. - N° de référence du client 20123147	**GETS Ref. No. - N° de réf. de SEAG** PW-$$XK-100-24691
File No. - N° de dossier 100xk.2B0KB-123147	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2012-08-30**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Menechian, Noubar	**Buyer Id - Id de l'acheteur** 100xk
Telephone No. - N° de téléphone (819) 956-4485 ( )	**FAX No. - N° de FAX** (819) 956-8303
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See herein	

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée See Herein	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N°de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

Issuing Office - Bureau de distribution

Secure Channel Division (XK)/Division de la voie de communication protégée (XK)
12C1, Place du Portage Phase III
11 Laurier St./11, rue Laurier
Gatineau
Québec
K1A 0S5

Canada

DEMANDE DE RENSEIGNEMENTS CONCERNANT LE

SERVICE DE SÉCURITÉ GÉRÉ DU GOUVERNEMENT DU CANADA (SSGGC)

POUR LE CANADA

TABLE DES MATIÈRES

A. 1 Contexte et objet 2
A. 2 Objectifs du service 3
A. 3 Hypothèses opérationnelles 3
A. 4 Exigences opérationnelles 3
A. 5 Modèle théorique 5
A. 6 Scénarios de déploiement possibles 6
A. 7 Objet de la présente demande de renseignements 6
A. 8 Nature de la demande de renseignements 6
A. 9 Nature et format des réponses attendues 6
A. 10 Coûts associés aux réponses 6
A. 11 Traitement des réponses 7
A. 12 Contenu de cette DDR 7
A. 13 Questions adressées à l'industrie 7
A. 14 Présentation matérielle des réponses 9
A. 15 Demandes de renseignements 10
A. 16 Présentation des réponses 10

Document joint

Ébauche de demande de proposition

A. 1 Contexte et objet

Services partagés Canada (SPC) offre actuellement aux ministères clients une suite de services de défense du périmètre entièrement gérés, y compris le portefeuille existant de services de sécurité gérés (SSG). Le portefeuille de SSG offre un ensemble complet de solutions visant la sécurité du périmètre, la détection des intrusions et le filtrage de contenu lié au Web et au courriel. Ces services peuvent être jumelés aux solutions existantes que possède le GC aux fins de protection globale des zones d'accès public des ministères.

L'acquisition des SSG se fait actuellement dans le cadre du contrat de la Voie de communication protégée qui prendra fin en décembre 2013. En conséquence, le lancement du présent projet d'acquisition d'un SSGGC a pour but de soumettre une nouvelle demande de soumissions concurrentielles à l'égard de ces services et d'amener les clients à effectuer la transition des SSG existants aux services du SSGGC d'ici décembre 2013.

L'architecture de déploiement des SSG est formée de solutions centralisées et distribuées, comme l'illustre la figure 1. Située dans le centre de données de l'entrepreneur, la solution centralisée offre au ministère client abonné les services d'antivirus et d'antipourriel en recourant aux politiques ministérielles en la matière. Cette solution est basée sur les appareils Cisco IronPort Email Security Appliances. La solution distribuée est située dans les zones d'accès public des ministères, à l'intérieur de leur centre de données. Elle s'appuie sur les serveurs Fortinet Fortigate et Cisco ASA UTM pour offrir les services de pare-feu et de détection des intrusions, et sur la solution de filtrage Web WebSense pour assurer le filtrage de contenu.

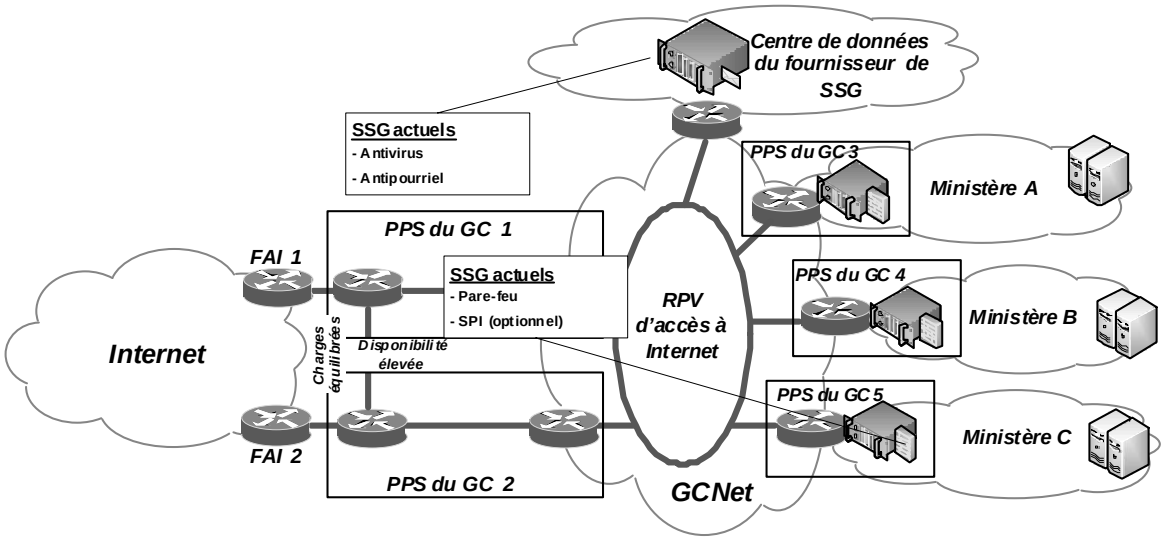

Figure 1 - Architecture de déploiement de SSG

A. 2 Objectifs du service

Le SSGGC vise les objectifs suivants :

(a) réduire les coûts opérationnels et administratifs;

(b) offrir un service extensible pour répondre à la demande;

(c) fournir un service protégé et privé conforme aux politiques en matière de sécurité et de protection des renseignements personnels;

(d) proposer une solution souple et polyvalente pour :

(i) s'adapter au changement constant du champ des menaces;

(ii) permettre plusieurs scénarios de déploiement;

(e) réduire les besoins en électricité et en superficie du centre de données;

(f) renforcer la sécurité grâce à l'adoption par les utilisateurs finals de comportements axés sur la sécurité.

A. 3 Hypothèses opérationnelles

Le SSGGC repose sur les hypothèses opérationnelles suivantes :

(a) le service doit être mis en œuvre dans les bureaux du GC indiqués par ce dernier;

(b) il doit permettre une transition en douceur des utilisateurs actuels des SSG;

(c) il doit être accrédité pour le traitement de renseignements de niveau « Protégé B »

(d) il n'y a pas de besoin pour de la formation avec instructeur.

A. 4 Exigences opérationnelles

SPC a besoin de remplacer le portefeuille existant du SSG par un SSGGC qui soit souple et agile, tout en tenant compte de ses exigences opérationnelles et techniques, et de l'évolution de l'industrie. Le SSGGC offrira aux ministères les services et l'infrastructure de TI qui permettront d'atténuer les risques de sécurité associés au raccordement à des réseaux non protégés et non fiables, tels qu'Internet, tout en renforçant la conformité aux politiques en matière de sécurité et d'utilisation, tel que l'indique le Secrétariat du Conseil du Trésor du Canada (SCT).

Le contrat qui résultera de cette démarche visera la prestation de services entièrement gérés pouvant comporter la mise en œuvre centralisée et distribuée des services de sécurité suivants :

- Pare-feu
- Prévention et détection des intrusions
- Filtrage de contenu
- Antivirus
- Antipourriel
- Gestion des informations et des événements de sécurité
- Prévention des pertes de données

Le contrat prévoira également des dispositions à l'égard des services sur demande qui appuient directement les services de sécurité susmentionnés, en l'occurrence :

- La formation de sensibilisation à la sécurité
- Le soutien à l'intégration

Le tableau qui suit décrit brièvement chacun des services du SSGGC.

Service de sécurité	Description
Pare-feu	Il agit comme un mécanisme de protection des actifs informationnels du Canada contre les menaces électroniques provenant de l'intérieur de gouvernement du Canada, ainsi que celles attribuables à la connexion à un réseau non fiable, tel Internet.
Prévention et détection des intrusions	La prévention et la détection des intrusions (PDI) surveillent le trafic réseau du Canada en temps réels en vue de déceler une activité hostile et d'alerter celui-ci dès que possible au sujet d'atteintes à la sécurité ou d'attaques organisées, et prennent les mesures appropriées.
Filtrage de contenu	Le filtrage de contenu balaie les demandes et le trafic Internet et peut empêcher l'accès à des sites et à du contenu Internet indésirables au moyen de politiques normalisées, appuyant ainsi la politique du Canada en matière d'utilisation acceptable.
Antivirus	L'antivirus assure une protection contre les codes malveillants en filtrant le trafic entrant et sortant afin de bloquer les fichiers infectés.
Antipourriel	L'antipourriel assure le captage des pourriels entrants et sortants en vue du filtrage et du blocage des tentatives d'hameçonnage.
Gestion des informations et des événements de sécurité	La gestion des informations et des événements de sécurité (GIES) collecte, analyse et corrèle l'information de journaux provenant de nombreuses sources à l'échelle de l'organisation, y compris de capteurs placés à des endroits stratégiques, afin de fournir des renseignements au sujet d'événements et d'incidents critiques liés à la sécurité tout en assurant l'établissement de documents et de rapports de nature judiciaire.
Prévention des pertes de données	La prévention des pertes de données (PPD) décèle, surveille et protège les données lors d'activités d'extrémité et de réseau afin de détecter et de prévenir toute transmission et utilisation non autorisées de renseignements confidentiels tout en renforçant les politiques internes connexes.

Tableau 1 - Services de sécurité gérés

Il convient de noter qu'on ne prévoit aucun chevauchement sur le plan des services entre le projet Initiative de transformation des services de courriels (ITSC) et le Service de sécurité géré du gouvernement du Canada (SSGGC). Le SSGGC vise à prolonger la durée de vie des services entièrement gérés existants de défense du périmètre fournis en vertu du contrat concernant la Voie de communication protégée, contrat qui prendra fin le 31 décembre 2013.

En lançant l'ITSC, Services partagés Canada (SPC) vise principalement à remplacer les systèmes de courriel actuels répartis entre les ministères partenaires de SPC par une solution de courriel consolidée. Compte tenu de la durée de vie prévue du contrat concernant le SSGGC et de la portée différente de celui ci, SPC ne prévoit pas tirer parti du SSGGC dans le cadre du projet ITSC.

A. 5 Modèle théorique

Le modèle théorique du SSGGC, illustré dans la figure 1, propose, à titre d'information seulement, une distribution des services de gestion des menaces qui est quelque peu semblable à celle adoptée par les services de sécurité gérés actuels. Les services de gestion des menaces sont répartis dans deux catégories :

(a) Les services hébergés centralement - sur des appareils partagés ou communs, à disponibilité élevée, situés à un point de contrôle Internet dont le Canada est propriétaire;

(b) Les services distribués - sur des appareils dédiés, standard ou à disponibilité élevée, situés dans les locaux de l'organisation cliente.

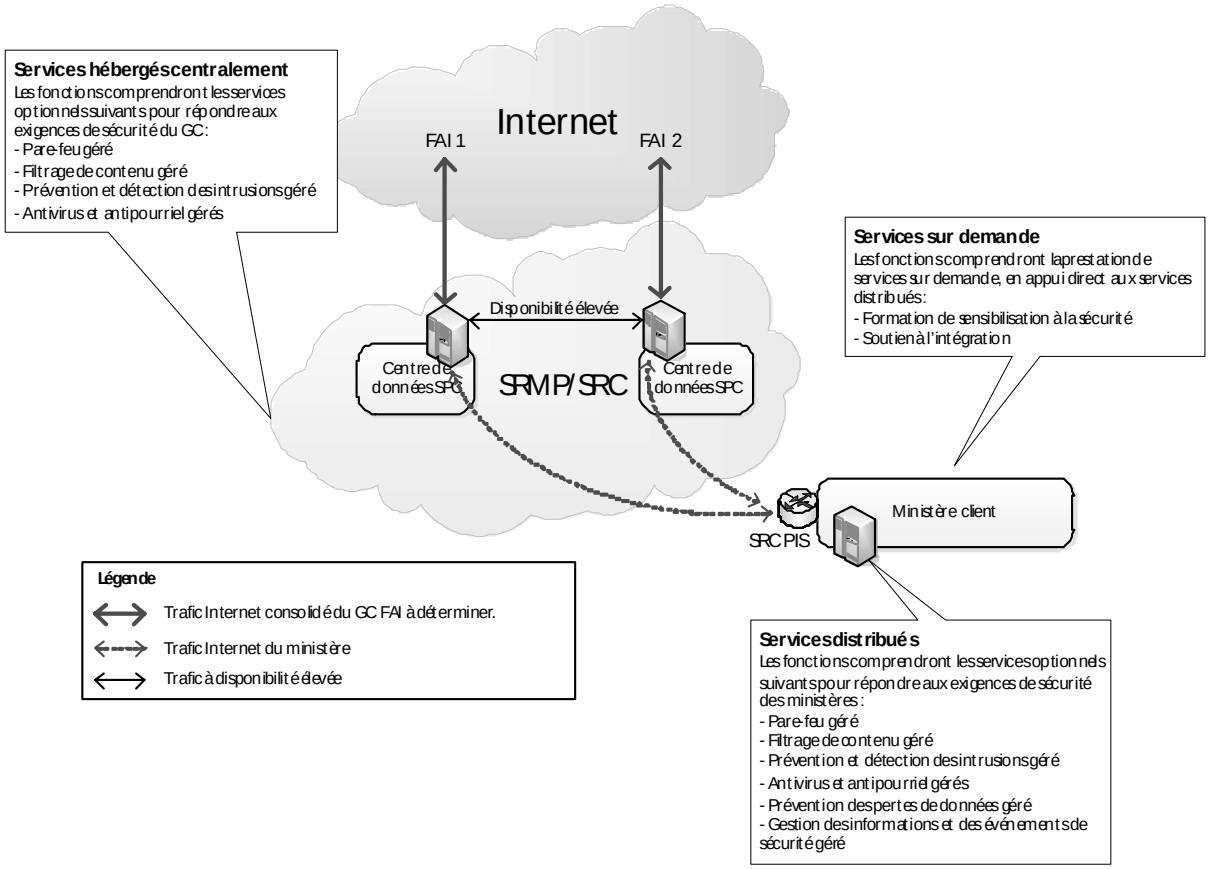

Figure 2 - Modèle théorique du SSGGC

Afin de faciliter la transition, tous les services de gestion des menaces doivent être en mesure de fonctionner les uns avec les autres, ainsi qu'avec les services de sécurité préexistants que possède l'organisation cliente et (ou) Services partagés Canada.

Chaque PPS centralisé doit avoir une capacité suffisante pour traiter tout le trafic Internet au cas où il y aurait perte d'un FAI (c'est-à-dire qu'il doit prendre en charge l'architecture d'accès Internet à disponibilité élevée).

A. 6 Scénarios de déploiement possibles

Le déploiement réel du SSGGC pourrait être réalisé en appliquant de multiples scénarios de déploiement. Le Canada a identifié trois scénarios qui pourraient permettre la mise en oeuvre du SSGGC tout en reconnaissant que l'approche distribuée conviendrait mieux à certaines organisations clientes, alors que l'approche centralisée serait mieux adaptée pour d'autres.

Pour de plus amples informations, veuillez consulter la pièce jointe 2.2 : Modèle de service.

A. 7 Objet de la présente demande de renseignements

La présente demande de renseignements vise à consulter l'industrie sur des points d'intérêt particuliers en lien avec la mise en œuvre du nouveau SSGGC. On demande à l'industrie de l'examiner et de nous soumettre toute indication supplémentaire ou rétroaction qui permettrait d'établir une demande de proposition juste et équitable.

A. 8 Nature de la demande de renseignements

Cette demande n'est pas un appel d'offres. Cette DDR ne donnera pas lieu à l'attribution d'un contrat. Par conséquent, les fournisseurs éventuels de tous biens ou services décrits dans cette DDR ne devraient pas réserver des stocks ou des installations, ni affecter des ressources en fonction des renseignements présentés dans cette DDR. Cette DDR ne donnera pas lieu non plus à l'établissement d'une liste de fournisseurs. Par conséquent, le fait qu'un fournisseur éventuel réponde ou non à cette DDR ne l'empêchera pas de participer à tout processus d'acquisition 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. Cette DDR vise seulement à obtenir les observations de l'industrie sur les points qui y sont abordés.

A. 9 Nature et format des réponses attendues

Les répondants sont invités à présenter leurs commentaires, préoccupations, et, le cas échéant, des recommandations pertinentes sur la façon de répondre aux besoins et aux objectifs définis dans cette DDR. Ils sont également invités à commenter le contenu, la forme et/ou le plan de tous documents préliminaires joints à cette DDR. Les répondants sont priés d'expliciter les hypothèses qu'ils avancent dans leur réponse.

A. 10 Coûts associés aux réponses

Le Canada ne remboursera pas les dépenses engagées pour répondre à cette DDR.

A. 11 Traitement des réponses

(a) **Utilisation des réponses :** Les réponses ne seront pas soumises à une évaluation officielle. Toutefois, le Canada pourra les utiliser pour élaborer ou modifier ses stratégies d'acquisition ou tous documents préliminaires joints à cette DDR. Le Canada examinera toutes les réponses reçues d'ici la date de clôture de la DDR. Cependant, s'il le juge opportun, il pourrait examiner les réponses reçues après la date de clôture de la DDR.

(b) **Équipe d'examen :** Une équipe d'examen composée de représentants du client (selon le cas) et de fonctionnaires de TPSGC examinera les réponses reçues. Ce dernier se réserve le droit d'engager des consultants indépendants ou de recourir aux services des ressources du gouvernement qu'il juge nécessaire pour examiner toute réponse. Toutes les réponses ne seront pas nécessairement soumises à l'examen de tous les membres de l'équipe d'examen.

(c) **Confidentialité** : Les répondants devraient indiquer les parties de leur réponse qu'ils jugent de nature exclusive ou confidentielle. Le Canada traitera les réponses selon les dispositions de la *Loi sur l'accès à l'information*.

(d) **Des séances individualisées d'activité de suivi** : Le Canada rencontrera tout répondant sur demande. Après la date de clôture, l'autorité contractante fera un suivi individuel auprès de tous les répondants qui auront indiqué dans leur réponse qu'ils désirent une rencontre avec le Canada.

A. 12 Contenu de cette DDR

(a) Cette DDR contient la demande de propositions provisoire et ses documents connexes, l'énoncé des travaux ainsi que les annexes et appendices. Ce document demeure un travail en cours et les répondants ne devraient pas présumer que des nouvelles dispositions ou exigences ne seront pas ajoutées à toute invitation à soumissionner qui, au bout du compte, pourrait être diffusée par le Canada. Les répondants ne devraient pas présumer non plus qu'aucune de celles-ci ne sera supprimée ou révisée. Des observations concernant ce document préliminaire seraient appréciées.

(b) Cette DDR contient également des questions précises à l'intention de l'industrie.

A. 13 Questions adressées à l'industrie

On demande aux entreprises de répondre aux questions figurant dans la présente section à la lumière de l'information soumises aux sections A1 à A6.

(a) **Question 1**

L'exécution des objectifs, des exigences opérationnelles, des hypothèses et du modèle théorique liés au SSGGC comporte-t-elle des obstacles ou risques? Veuillez commenter.

(b) **Question 2**

La solution que vous proposez se compare-t-elle aux services commerciaux que vous offrez actuellement, sur le plan des objectifs et exigences opérationnelles? Veuillez commenter.

(c) **Question 3**

Pour faciliter la gestion opérationnelle tout en minimisant les coûts généraux, le Canada doit compter sur un modèle de tarification qui serait basé sur un prix unique d'installation du service à un site donné, un prix unique par fonction et de faibles versements périodiques. Selon vous, s'agit-il d'une approche viable? D'autres solutions commerciales et/ou rentables pourraient-elles s'appliquer? Veuillez commenter.

(d) **Question 4**

Pour faciliter le déploiement de nouveaux sites et la mise à niveau des sites existants par l'ajout de fonctions, le Canada exige que le service puisse fonctionner à vitesse filaire lorsque toutes les fonctions possibles sont sollicitées. Selon vous, s'agit-il d'une approche viable? D'autres solutions commerciales et/ou rentables pourraient-elles s'appliquer? Veuillez commenter.

(e) **Question 5**

Veuillez indiquer comment le portail de rapports que vous proposez s'harmonise avec les solutions commerciales disponibles, appuie les mécanismes de rapport connexes comme les serveurs Syslog et s'intègre aux procédures de communication du Centre de protection de l'information.

Quelle est l'ampleur des mesures d'adaptation que nécessite la solution que vous proposez pour qu'elle soit prête sur le plan commercial?

(f) **Question 6**

Veuillez indiquer comment le service géré que vous proposez assurerait une gestion, intrabande et hors bande, à distance sécurisée des solutions qui, logiquement, pourraient être déployées dans des zones d'accès publiques et/ou opérationnelles.

(g) **Question 7**

Veuillez indiquer comment le service de gestion des informations et des événements de sécurité que vous proposez se compare aux services commerciaux que vous offrez.

Quelle est l'ampleur des mesures d'adaptation que nécessite la solution que vous proposez pour qu'elle soit prête sur le plan commercial?

(h) **Question 8**

Veuillez indiquer comment le service de prévention des pertes de données que vous proposez se compare aux services commerciaux que vous offrez.

Quelle est l'ampleur des mesures d'adaptation que nécessite la solution que vous proposez pour qu'elle soit prête sur le plan commercial?

(i) **Question 9**

Veuillez indiquer comment le service géré de formation de sensibilisation à la sécurité que vous proposez se compare aux services commerciaux que vous offrez.

Quelle est l'ampleur des mesures d'adaptation que nécessite la solution que vous proposez pour qu'elle soit prête sur le plan commercial?

(j) **Question 10**

En présumant que le Canada exécute à la fois les services IPv4 et IPv6, veuillez indiquer comment votre solution se démarque par rapport aux aspects suivants :

(i) Fonctionnalités d'IPv6 (p. ex. BCP 38, RFC 3704)

(ii) Lacunes sur le plan du service entre IPv4 et IPv6

(iii) Problème d'interopérabilité d'IPv6 dans le contexte d'une solution faisant appel à de multiples fournisseurs (composantes/pièces/boitiers) et du réseau du Canada

(iv) Différences sur le plan de la performance entre les services d'IPv6 et d'IPv4

(v) Mécanismes de transitions d'IPv4 à IPv6 : traduction et tunnellisation

(k) **Question 11**

Le US National Information Assurance Partnership (NIAP) compte un programme, soit le Common Criteria Evaluation and Validation Scheme (CCEVS), permettant d'évaluer la conformité des produits de TI par rapport aux normes internationales. Le NIAP est en voie de remplacer les niveaux d'assurance de l'évaluation existants par de nouveaux profils de protection (PP) propres à une technologie déterminée. Ces nouveaux PP sont en cours d'élaboration et ne seront pas disponibles avant la fin de 2012.

Dans ce contexte, veuillez indiquer comment vous comptez vous assurer que votre fabricant d'équipement d'origine s'engagera à certifier ses produits par rapport aux PP approuvés par le NIAP, à mesure que ceux-ci deviendront disponibles, afin qu'ils paraissent sur la liste des produits conformes.

Veuillez indiquer comment le Canada pourrait traiter, dans l'Énoncé des travaux au SSGGC, de la question du moment opportun de la certification des produits par rapport aux PP à venir.

(l) **Question 12**

Tel que publié sur Merx (no : 2B0KB-12NNSE/A) le 28 mai dernier, SPC prévoit invoquer l'exception relative à la sécurité nationale en ce qui concerne les marchés publics de SPC liés aux réseaux et aux télécommunications. Étant donnée l'importance du service pour la sécurité nationale du Canada, ces derniers devraient inclure le SSGGC. Veuillez commenter sur les exigences du SSGGC par rapport à l'exception relative à la sécurité nationale :

(i) La propriété et le contrôle des soumissionnaires, ainsi que leurs sous-traitants, doivent être canadiens à 100%.

(ii) Les bases de données doivent êtres situées exclusivement au Canada et le trafic de réseau doit être acheminé exclusivement à l'intérieur du Canada.

(iii) Les produits commerciaux qui font partie du service doivent être approuvés par le Centre de la sécurité des télécommunications Canada.

(m) **Question 13**

Veuillez indiquer comment il serait possible d'étendre aux appareils mobiles les services de sécurité géré que vous proposez. Dans quelle mesure faudrait-il personnaliser la solution que vous proposez pour qu'elle soit prête sur le plan commercial?

A. 14 Présentation matérielle des réponses

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

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

(i) le titre de la réponse du répondant et le numéro du volume;

(ii) le nom et l'adresse du répondant;

(iii) le nom, l'adresse et le numéro de téléphone de la personne-ressource du répondant;

(iv) la date;

(v) le numéro de la DDR.

(c) **Système de numérotation :** Les répondants sont priés d'utiliser dans leur réponse un système de numérotation correspondant à celui de cette DDR. Toute référence à des documents descriptifs, à des manuels techniques et à des brochures accompagnant la réponse devrait respecter ce système.

(d) **Nombre de copies :** Le Canada demande aux entreprises qui présenteront une réponse de soumettre deux copies sur papier et une copie électronique.

A. 15 Demandes de renseignements

Comme il ne s'agit pas d'un appel d'offres, le Canada ne répondra pas nécessairement aux demandes de renseignements écrites des fournisseurs ou ne distribuera pas nécessairement 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 : Noubar Menechian

Courriel : noubar.menechian@spc-ssc.gc.ca

Téléphone : (819) 956-4485

Télécopieur : (819) 956-5165

A. 16 Présentation des réponses

(a) **Délai de présentation des réponses et adresse d'expédition :** Les fournisseurs intéressés devraient envoyer leur réponse à l'adresse suivante et s'assurer qu'elle est reçue d'ici l'heure et la date indiquées à la page 1 de ce document :

Unité de réception des soumissions
Place du Portage, Phase III, 0A1
11, rue Laurier
Gatineau (Québec) K1A 0S5

Télécopieur : (819) 997-9776

Veuillez ne pas adresser votre réponse à l'autorité contractante.

(b) **Responsabilité en ce qui a trait à la réception des réponses dans les délais prescrits :** Il incombe à chaque répondant de s'assurer que sa réponse est livrée à la bonne adresse et qu'elle est reçue dans les délais prescrits.

(c) **Adresse de l'Unité de réception des soumissions à la seule fin de livraison des réponses :** Aucun autre document ne doit être envoyé à cette adresse.

(d) **Identification des réponses :** Chaque répondant devrait s'assurer que son nom et son adresse, le numéro de la DDR et la date de clôture figurent lisiblement sur l'enveloppe.