RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0A1/ Noyau 0A1
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Linguistic Services Division / Division des services linguistiques
PSBID, PWGSC / DIASP,TPSGC
11 Laurier St. / 11, rue Laurier
10C1/Place du Portage, Phase III
Gatineau
Québec
K1A 0S5

Title - Sujet RFI - CITIZENSHIP KNOWLEDGE E-TEST.	
Solicitation No. - N° de l'invitation B9514-120390/A	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client B9514-120390	**Date** 2013-04-22
GETS Reference No. - N° de référence de SEAG PW-$$ZF-504-25980	
File No. - N° de dossier 504zf.B9514-120390	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2013-05-22**	**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: Cardinal, France	**Buyer Id - Id de l'acheteur** 504zf
Telephone No. - N° de téléphone (819) 956-1778 ( )	**FAX No. - N° de FAX** (819) 956-9235
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**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**	

La présente modification est émise afin d'inclure l'annexe C de la pièce jointe 1 de la Demande de renseignements (DDR).

Il n'y a aucune modification au document anglais.

TOUTES LES AUTRES CONDITIONS DEMEURENT INCHANGÉES

ANNEXE C
EXIGENCES RELATIVES À LA SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

1. Exigences relatives à la sécurité de la technologie de l'information

1.1 Sécurité relative à la technologie de l'information

Le fournisseur doit :

a) protéger les bases de données ou les systèmes informatiques qui emmagasinent les renseignements personnels contre un accès non autorisé par des méthodes couramment utilisées conformes ou supérieures aux normes de l'industrie, notamment :

   i) des contrôles d'authentification et d'autorisation;
   ii) la défense du périmètre - pare-feu;
   iii) détection des intrusions;
   iv) segmentation du réseau;
   v) désactivation de l'accès aux supports amovibles de l'ordinateur, tels que les ports USB, la connexion sans fil, les disques durs externes, les lecteurs optiques, la connexion Bluetooth.

b) veiller à ce que les données d'essai et les renseignements sur les clients soient stockées sur des serveurs appartenant à des entreprises canadiennes et empêcher que de l'information ne franchisse les frontières du territoire canadien.

1.2 Registres de vérification et événements

Le fournisseur doit :

a) tenir à jour des registres de vérification où est consigné électroniquement chaque accès ou tentative d'accès aux dossiers de renseignements personnels stockés électroniquement;
b) veiller à ce que les registres de vérification soient présentés de façon telle que le fournisseur et le responsable de projet puissent les consulter en tout temps;
c) veiller à ce que les registres de vérification contiennent les renseignements suivants :

   i) l'entité à l'origine de l'événement (p. ex.. le nom de l'utilisateur);
   ii) la date et l'heure de l'événement;
   iii) le type d'événement;
   iv) un identificateur unique de l'événement visant le dossier ou l'ensemble de données qui a été manipulé;
   v) l'état des résultats (s'il y a lieu);
   vi) l'identificateur unique de la machine associée à l'événement;
   vii) l'identificateur unique de l'emplacement de l'événement.

d) conserver en toute sécurité les registres de vérification pendant au moins six (6) mois;
e) remettre les registres de vérification au responsable de projet qui en fait la demande.

1.3 Authentification des données et autorisation

Le fournisseur doit :

a) stocker électroniquement les renseignements personnels de manière qui requiert un mot de passe (ou un mécanisme de contrôle de l'accès similaire) pour accéder au système ou à la base de données où cette information est conservée;
b) veiller à ce que les mots de passe et tout autre mécanisme de contrôle de l'accès soit confié aux seuls employés qui ont besoin d'accéder à ces renseignements personnels pour faire leur travail et qui ont obtenu l'autorisation nécessaire du responsable de projet;
c) mettre en application des mots de passe robustes qui bloquent l'accès après un nombre paramétrable de tentatives infructueuses et qui comportent au moins huit (8) caractères, dont :

    i) au moins une (1) majuscule (A à Z);
    ii) au moins une (1) minuscule (a à z);
    iii) au moins un (1) caractère autre qu'une lettre ou un chiffre (p. ex., %, +, @ ou !);
    iv) au moins deux (2) chiffres (0 à 9).

d) veiller à ce que le compte de l'employé soit fermé rapidement lorsque ce dernier quitte ses fonctions.

1.4 Sauvegarde et récupération

Le fournisseur doit :

a) maintenir en place une routine de sauvegarde sécurisée de tous les renseignements personnels;
b) veiller à ce que les renseignements recueillis et tenus à jour ne soient pas stockés :

    i) dans un environnement de stockage de données en " nuage ";
    ii) sur des supports de stockage amovibles et non chiffrés (disquettes, dispositifs USB, etc.).

1.5 Exigences relatives à la protection contre les programmes malveillants

Le fournisseur doit :

a) installer les logiciels de protection contre les programmes malveillants, qui sont conformes ou supérieurs aux normes de l'industrie sur tous les systèmes informatiques utilisés pour réaliser les travaux dans l'exécution des travaux prévus au présent contrat;
b) veiller à ce qu'une analyse des systèmes informatiques au moyen de logiciels antivirus soit effectuée chaque jour en utilisant les définitions de virus mises à jour quotidiennement.

1.6 Exigences relatives à la sécurité du réseau

Le fournisseur doit :

a) veiller à ce qu'il soit impossible d'accéder directement au moyen d'une connexion Internet aux systèmes informatiques utilisés dans le cadre de l'exécution des travaux prévus au présent contrat;
b) recourir aux algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications Canada (CSTC) pour assurer la protection des renseignements cotés " Protégé B " dans l'éventualité où il aura besoin d'utiliser un mécanisme de chiffrement pour garantir la sécurité des renseignements personnels (http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-fra.html).

1.7 Autres exigences relatives à la sécurité informatique

Le fournisseur doit :

a) installer régulièrement les correctifs de sécurité recommandés par le fournisseur du système d'exploitation et des applications sur toutes les plateformes informatiques utilisées dans le cadre de l'exécution des travaux prévus au présent contrat;
b) tenir à jour des registres détaillés faisant état des modifications apportées aux systèmes informatiques qui traitent ou servent à stocker des renseignements personnels;
c) fournir les registres des modifications et de gestion de la configuration aux responsables des clients qui en font la demande;
d) renforcer les plateformes informatiques utilisées dans le cadre de l'exécution des travaux prévus au présent contrat en vue de les rendre conformes ou supérieures aux normes de l'industrie.

1.8 Exigences relatives à la sécurité de la gestion de l'information

Le fournisseur doit :

a) élaborer une sécurité en matière de sécurité et un ensemble de consignes de sécurité opérationnelle en rapport avec les travaux dont l'exécution est prévue au présent contrat;
b) fournir cette politique et ces consignes à l'autorité contractante qui en fait la demande;
c) élaborer et remettre à l'autorité contractante un plan de sécurité qui comprend notamment :

    i) la description des rôles et responsabilités de l'entrepreneur en matière de sécurité;
    ii) la description du processus de filtrage de la sécurité du personnel de l'entrepreneur et les mesures afférentes de protection du personnel;
    iii) la description des mesures matérielles de protection;
    iv) la description du programme de sensibilisation à la sécurité de l'entrepreneur;
    v) la description du programme de gestion de la configuration de l'entrepreneur;

vi) la description des mesures de protection informatique de l'entrepreneur (p. ex., pare-feu, systèmes d'authentification et d'autorisation);
vii) la description de la planification des mesures d'urgence de l'entrepreneur;
viii) la description des processus d'intervention en cas d'incidents liés à la sécurité de l'entrepreneur;
ix) la description du programme de vérification et de reddition de comptes de l'entrepreneur;
x) la description des processus internes de vérification et d'atténuation des risques de l'entrepreneur;
xi) la description du processus de renforcement de la sécurité de l'entrepreneur;
xii) la description du processus d'installation des correctifs du système d'exploitation et des applications de l'entrepreneur;
xiii) la description des pratiques et de normes de renforcement de l'entrepreneur;
xiv) la description des mesures de protection à proximité des contenants et la gestion des clés et combinaisons de l'entrepreneur.

d) identifier ou marquer les renseignements personnels comme suit :

i) tous les documents imprimés contenant des renseignements personnels doivent porter la mention " PROTÉGÉ B " inscrite en lettres majuscules dans le coin supérieur droit du côté recto. Dans la mesure du possible, la même exigence s'applique aux supports de stockage chiffrés, fixes ou amovibles, qui contiennent des renseignements personnels, comme les disquettes, les disques durs (internes et externes), les cartes de mémoires et les écrans. Dans ce cas, la mention " PROTÉGÉ B " est apposée sur la surface externe du dispositif de stockage et doit être intelligible et lisible à l'œil nu;

e) à la demande du responsable de projet, fournir tous les renseignements raisonnables et pertinents dont il a besoin pour réaliser une analyse des menaces et des risques. Ces renseignements comprennent notamment :

i) les différentes politiques et procédures;
ii) le plan de sécurité;
iii) le plan d'intervention en cas d'urgence;
iv) les registres des systèmes informatiques de traitement et de stockage des renseignements personnels des Canadiens;
v) les rapports d'évaluation des vulnérabilités;
vi) les rapports d'essai de pénétration;
vii) les rapports sur les autorisations accordées aux utilisateurs;

f) à intervalles réguliers, examiner la situation liée à la sécurité et communiquer les résultats au responsable. Cet examen doit comporter au moins les volets suivants :

i) la réévaluation des menaces locales à la sécurité au moins une fois l'an ou à la suite d'un changement important;
ii) l'examen de la sécurité à la suite d'un incident grave lié à la sécurité;

iii) une évaluation des vulnérabilités des hôtes hébergeant les systèmes, au moins une fois l'an;
iv) la mise à l'essai des mesures de protection contre la pénétration du périmètre, au moins une fois l'an;
v) la vérification, à l'interne ou par un tiers, des processus et des procédures de sécurité, au moins une fois l'an;

g) procéder à l'examen des systèmes informatiques et passer manuellement en revue les registres, au moins une fois par semaine.

1.9 Gestion des incidents liés à la sécurité informatique

Le fournisseur doit :

a) élaborer un plan d'intervention en cas d'urgence pour répondre à diverses situations d'urgence (p. ex., incendie, alerte à la bombe, catastrophe naturelle, etc.);
b) veiller à ce que le plan d'intervention en cas d'urgence prévoit la façon dont l'information et les biens sont protégés dans de telles situations;
c) informer sur-le-champ le responsable de projet des atteintes à la sécurité ou des incidents liés à cette dernière qui surviennent dans le cadre de l'exécution des travaux prévus au présent contrat, notamment :

i) l'accès non autorisé aux renseignements personnels, ainsi que leur utilisation ou leur divulgation sans autorisation;
ii) les incidents susceptibles de compromettre la sécurité ou l'intégrité de l'information;
iii) les actes illégaux (vol de enseignements, allégations de corruption ou de chantage);
iv) les alertes à la bombe;
v) les urgences incendie;
vi) les agressions physiques;
vii) les menaces (verbales, écrites ou au téléphone);
viii) les entrées par effraction;
ix) les manifestations et l'occupation illégale des lieux;
x) le actes de vandalisme;
xi) le vol (biens et articles répertoriés);
xii) les dommages et les pertes (biens matériels);
xiii) les maliciels (p. ex., virus);
xiv) les atteintes à la sécurité informatique;
xv) l'altération des contenants de sécurité;

d) dans les limites du raisonnable, prendre sur-le-champ toutes les mesures nécessaires pour résoudre le problème et empêcher qu'il ne se reproduise, ainsi qu'appliquer les mesures demandées par l'autorité contractante.

1.10 Rapports sur la sécurité

Le fournisseur doit :

a) dans les 30 jours après la fin de l'année civile, remettre à l'autorité contractante un exemplaire du rapport annuel sur la sécurité de chaque emplacement et qui contient au moins les éléments d'information suivants :

   i) la ou les copies de toutes les versions à jour des formulaires de demande de consentement qu'utilise l'entrepreneur pour recueillir des renseignements personnels;
   ii) la liste des types de renseignements personnels que l'entrepreneur a recueillis et utilisés et qui ont trait aux travaux exécutés;
   iii) la liste exhaustive des emplacements où sont stockées des copies imprimées des renseignements personnels;
   iv) la liste exhaustive des emplacements où sont stockés des renseignements personnels sous forme lisible par machine (p. ex., l'emplacement où se trouve un serveur qui héberge une base de données comprenant des renseignements personnels de toute nature), y compris les sauvegardes;
   v) la liste exhaustive des personnes auxquelles l'entrepreneur a accordé un droit d'accès à des renseignements personnels;
   vi) la liste exhaustive des mesures de protection appliquées par l'entrepreneur pour protéger les renseignements personnels;
   vii) la liste exhaustive et la description détaillée des menaces potentielles ou réelles auxquelles sont exposés les renseignements personnels, ainsi que l'évaluation des risques qui découlent de ces menaces et le caractère approprié des mesures de protection contre ces risques;
   viii) liste exhaustive et la description détaillée des nouvelles mesures de protection que l'entrepreneur entend appliquer pour protéger les renseignements personnels durant la prochaine année;

b) écraser les données électroniques que contiennent les supports de stockage au moyen d'un logiciel d'effacement sécurisé approuvé dont le nom apparaît dans le Bulletin de sécurité des technologies de l'information, émis par la sous-direction de la sécurité technique de la GRC (http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/b2-002-fra.pdf).