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 0B2 / Noyau 0B2
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

Title - Sujet Carnets de document d'aviation	
Solicitation No. - N° de l'invitation T8518-130090/B	**Amendment No. - N° modif.** 010
Client Reference No. - N° de référence du client T8518-130090	**Date** 2015-02-06
GETS Reference No. - N° de référence de SEAG PW-$$CW-010-66268	
File No. - N° de dossier cw010.T8518-130090	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2015-02-12**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Gagné-Templeman, Kathleen	**Buyer Id - Id de l'acheteur** cw010
Telephone No. - N° de téléphone (613) 990-9189 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

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

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**

Issuing Office - Bureau de distribution

Communication Procurement Directorate/Direction de l'approvisionnement en communication
360 Albert St./ 360, rue Albert
12th Floor / 12ième étage
Ottawa
Ontario
K1A 0S5

Canada

Le but de cette modification est d'apporter les révisions suivantes :

1) À la Modification 008 - PARTIE A – RÉPONDRE AUX QUESTIONS DES SOUMISSIONNAIRES

SUPPRIMER intégralement la PARTIE A ET LA REMPLACER par la suivante :

Question 28 :

Modification 002
Annexe C - Document technique sur les exigences en matière de sécurité des TI **– Point 7**

Devrait-on lire « *documents de nature* PROTÉGÉS » plutôt que « *documents de nature délicate* »?

Réponse 28 :

Document technique sur les exigences en matière de sécurité des TI **– Point 7**

Le document sur la sécurité des TI a fait l'objet d'une révision. Prière de se rapporter à la Partie 2 de cette modification apportée à la présente DP.

Question 29 :

Modification 002
Annexe C - Document technique sur les exigences en matière de sécurité des TI **– Point 15**

a) On retrouve dans cette section les termes « *renseignement de nature délicate » et «* agents », qui n'ont pas été définis auparavant. Ces termes devraient-ils être respectivement remplacés par les termes « PROTÉGÉS » et « sous-traitants »?

b) Cette section exige que l'entrepreneur remette ou supprime tous les renseignements PROTÉGÉS en sa possession à la fin du contrat. L'entrepreneur a l'obligation de tenir des registres en vertu des clauses du Guide des CCUA 2030 33 (2014-09-25) Comptes et vérification et 2030 12 (2014-09-25) Inspection et acceptation des travaux. Est-ce que TCAC/TPSGC peut confirmer que l'entrepreneur peut inclure dans les registres les renseignements PROTÉGÉS B comme l'exige le contrat?

Réponse 29 :

Modification 002
Document technique sur les exigences en matière de sécurité des TI **– Point 15**

a. Le document sur la sécurité des TI a fait l'objet d'une révision. Prière de se rapporter à la Partie 2 de cette modification apportée à la présente DP.

b. Le soumissionnaire doit tenir les dossiers à jour, tel que décrit aux conditions du contrat énoncées aux conditions générales 2030 33 et 2030 12 (25/09/2014) et conformément aux exigences du contrat relatives à la sécurité.

Question 30 :

Modification 002
Annexe C - Document technique sur les exigences en matière de sécurité des TI **– Point 18**

Cette section ne fait référence qu'au « disque dur de l'ordinateur ». Devrait-on plutôt y lire, comme dans la section 15 (noté précédemment), « tout dispositif de stockage » (p. ex., disques SSD, DVD, cassettes, clés USB, etc.)?

Réponse 30 :

Modification 002
Document technique sur les exigences en matière de sécurité des TI **– Point 18**

Le document sur la sécurité des TI a fait l'objet d'une révision. Prière de se rapporter à la Partie 2 de cette modification apportée à la présente DP.

Question 31 :

Modification 002
Annexe C – Document technique sur les exigences en matière de sécurité des TI **– Point 18**

La pratique établie, approuvée par la DSIC, consiste à détruire à l'interne tous les supports de données, conformément aux pratiques approuvées par la DSIC. De nombreux dispositifs de l'entreprise sont utilisés pour de multiples projets du gouvernement du Canada et bien que les données puissent être classées de façon logique, elles pourraient être sur des supports distincts. Remettre à TC un support de données qui a été utilisé pour un autre contrat du gouvernement du Canada est problématique. Pour se conformer à cette exigence, l'entreprise devrait probablement acheter des serveurs distincts et d'autres appareils de stockage de données pour TC (ce qui représenterait un coût beaucoup plus élevé pour TCAC).

Serait-il acceptable de suivre les pratiques approuvées par la DSIC par le passé?

Réponse 31 :

Le document sur la sécurité des TI a fait l'objet d'une révision. Prière de se rapporter à la Partie 2 de cette modification apportée à la présente DP.

PARTIE 2) Modification 002
ANNEXE C - **SUPPRIMER intégralement le *Document technique sur les exigences en matière de sécurité des TI*,** *Carnet de documents d'aviation (CDA), Transports Canada* **ET LE REMPLACER par le document suivant :**

Guide de sécurité pour entrepreneurs qui utilisent les installations et le matériel informatique pour la production, le stockage et le traitement de renseignements électroniques protégés cotés B et pour l'accès à ces renseignements.

(le document suit cette page)

TOUTES LES AUTRES MODALITÉS ET CONDITIONS DEMEURENT INCHANGÉES

Guide de sécurité pour entrepreneurs qui utilisent les installations et le matériel informatique pour la production, le stockage et le traitement de renseignements électroniques protégés cotés B et pour l'accès à ces renseignements.

Exigences en matière de gestion de la sécurité des technologies de l'information (STI)

(Niveau de sensibilité maximal – « Protégé B »

Les entrepreneurs de Transport Canada (TC) qui utilisent leurs installations et leur matériel informatique pour traiter, stocker des renseignements confidentiels protégés cotés B, et pour y avoir accès, sont tenus d'observer les critères ci-après et des renseignements détaillés sur la configuration STI de leurs systèmes et de leurs installations aux services de GI/TI de Transport Canada.

Exigences :

1. Les entrepreneurs doivent autoriser Transport Canada (TC) à effectuer l'inspection et la vérification de l'infrastructure en technologie de l'information si nécessaire.

2. Employés des partenaires ou des tierces parties
   2.1. Les employés (y compris les entrepreneurs) qui ont accès à des renseignements protégés cotés B ou qui fournissent des services administratifs, de soutien ou de maintenance pour l'infrastructure en technologie de l'information ou ses produits d'information doivent posséder une cote d'autorisation de vérification de fiabilité approfondie minimale, en conformité avec la Norme sur la sécurité du personnel du Secrétariat du Conseil du Trésor.

3. Les entrepreneurs doivent observer les mesures de contrôle administratives, les concepts et la philosophie de gestion du risque énoncés dans la Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information (GSTI) :
   3.1. Modification des processus de contrôle et de gestion visant l'approbation des changements apportés au matériel et aux logiciels.
   3.2. Gestion de la configuration – définie et documentée.
   3.3. Tenue du registre de la maintenance et des modifications apportées aux services et aux systèmes connexes.
   3.4. Surveillance des systèmes de renseignements protégés cotés B et signalement d'accès compromis ou non autorisé par TC aux fonds de renseignements.

4. Utilisez les contrôles techniques et les concepts d'exploitation suivants (s'il y a lieu) :
   4.1. Contrôle de l'accès – permet d'éviter tout accès non autorisé. Utiliser des procédures définies pour autoriser, révoquer et surveiller l'accès.
   4.2. Mots de passe fiables – utiliser un minimum de huit caractères, adopter des règles complexes (caractères alphanumériques, spéciaux, majuscules et minuscules), conserver l'historique des mots de passe, apporter des changements à intervalles réguliers et utiliser des règles de verrouillage).
   4.3. Accès à l'information en fonction du rôle de l'utilisateur – appuyer le principe du « privilège minimal ».
   4.4. Expiration de session – fournir un délai raisonnable d'expiration de la session pour les systèmes d'exploitation et les applications.
   4.5. Règle d'utilisation du système – définir ce qui constitue une utilisation acceptable et un niveau de sensibilité acceptable de l'information.
   4.6. Sécurité de la communication des données – le transfert de données entre les divers systèmes et les interfaces d'utilisateurs finaux comme IPSec, SSL/TLS (les produits cryptographiques et les algorithmes doivent être approuvés par le Centre de la sécurité des télécommunications

Canada (CSTC), le National Institute of Standards and Technology (NIST) et le Federal Information Processing Standard (FIPS).

4.7. Sécurité du stockage des données – les données inactives doivent être encodées (les produits cryptographiques et les algorithmes doivent être approuvés par le CSTC et être conformes au NIST et au FIPS).
4.8. Segmentation de réseau pour les serveurs et les bases de données protégés cotés B – utiliser différentes zones de réseau pour séparer les postes de travail des clients, des serveurs d'application et des bases de données au moyen de pare-feu entre les zones et par le filtrage et l'imposition de restrictions d'accès et de circulation.
4.9. Infrastructure de sécurité – utiliser des pare-feu et des mesures de prévention et de détection des intrusions, des codes malveillants entre les réseaux publics et privés (à la frontière et dans le périmètre du réseau).
4.10. Enregistrement des activités – suivre de près les accès utilisateur, les registres d'activité (les tentatives de connexion infructueuses).
4.11. Gestion des correctifs et mises à jour de sécurité – appliquer ces mesures rapidement et à intervalle régulier.
4.12. Réseautage sans fil – employer une solide authentification et des normes de chiffrage de données.
4.13. Gestion de sauvegarde – encoder et conserver les sauvegardes de façon sécuritaire.
4.14. Ségrégation des données du client – conserver les données des clients séparément les uns des autres.
4.15. Planification des mesures d'urgence – élaborer des plans raisonnables de récupération des données.

5. Éliminer toutes les données électroniques qui contiennent ou qui ont contenu des renseignements protégés cotés B, conformément aux exigences du CSTC et de la GRC, lorsque le matériel est remplacé, mis à niveau ou lorsqu'un service est interruption ou lorsque Transport Canada en fait la demande.

6. Recommandations et pratiques exemplaires :
   6.1. Effectuer des évaluations de la menace et du risque pour les applications et l'infrastructure TI.
   6.2. Mettre en œuvre une politique d'utilisation acceptable du réseau.
   6.3. Établir des normes officielles et des exigences de sécurité de base pour les logiciels et le matériel approuvé.
   6.4. Effectuer des évaluations de la vulnérabilité sur une base régulière
   6.5. Utiliser l'authentification à deux facteurs pour les accès administrateur et utilisateur privilégié.
   6.6. Recourir à des pratiques de sécurité exemplaires lors de l'élaboration d'applications personnalisées.
   6.7. Appliquer des pratiques de sécurité exemplaires lors de la configuration de logiciel et de matériel.
   6.8. Appliquer les recommandations du NIST SP-800-53 REV 3.