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

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

Title - Sujet IMPRESSION VARIABLE - T4 001TAX	
Solicitation No. - N° de l'invitation G8034-120005/A	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client G8034-120005	**Date** 2013-08-09
GETS Reference No. - N° de référence de SEAG PW-$$CW-010-63198	
File No. - N° de dossier cw020.G8034-120005	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2013-08-28**	**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: Werk, Janet	**Buyer Id - Id de l'acheteur** cw020
Telephone No. - N° de téléphone (613) 998-3968 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** see herein	

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**

Cette modification a pour but de joindre le document << Exigences relatives à la sécurité des technologies de l'information >>

Tous les autres termes et conditions demeurent inchangées.

Document technique sur les exigences en matière de sécurité des TI Sécurité des TI, Ressources humaines et Développement des compétences Canada

Les exigences en matière de sécurité de Ressources humaines et Développement des compétences Canada (RHDCC) pour le contrat susmentionné sont celles incluses dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

En outre, il faut également tenir compte des exigences additionnelles suivantes :

1. Chaque entrepreneur qui demande l'accès à des renseignements PROTÉGÉS doit détenir une COTE DE FIABILITÉ valide, octroyée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

2. L'entrepreneur ne doit pas donner accès aux renseignements de RHDCC à des sous-traitants, à des bénévoles, à des délinquants ou à d'autres parties, à moins que ces personnes aient été autorisées par RHDCC, qu'elles détiennent une COTE DE FIABILITÉ valide et qu'elles aient un besoin légitime de connaître les renseignements fournis par le système.

3. L'entrepreneur ne doit pas donner aux personnes qui ne détiennent pas de COTE DE FIABILITÉ accès à des ordinateurs qui sont utilisés ou qui ont été utilisés pour traiter les renseignements de RHDCC, ni leur permettre d'aider à réparer ou à exploiter des systèmes informatiques utilisés pour accéder aux renseignements de RHDCC.

4. L'entrepreneur doit s'assurer que tous ses employés qui prennent part à l'exécution du contrat connaissent parfaitement leurs obligations en matière de sécurité relativement au traitement des renseignements PROTÉGÉS.

5. Si des renseignements PROTÉGÉS sont stockés ou traités sur un ordinateur appartenant à l'entrepreneur ou sur des supports informatiques amovibles tels qu'une clé USB, ces renseignements doivent être protégés à l'aide d'un mot de passe fort et chiffrés à l'aide d'un produit conforme à la norme FIPS 140-2.

6. L'entrepreneur ne doit utiliser les ordinateurs destinés à l'exécution du contrat que dans une zone d'utilisation conforme à la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor.

7. L'entrepreneur doit, lorsqu'il ne les utilise pas, mettre en lieu sûr dans un coffre de sécurité approuvé par la GRC tous les documents de nature délicate stockés sur des supports informatiques amovibles.

8. L'entrepreneur doit s'assurer que l'écran et le matériel imprimé ne sont pas visibles par des personnes non autorisées.

9. L'entrepreneur transportant tout renseignement PROTÉGÉ doit utiliser une sacoche à documents verrouillée approuvée par la GRC (c.-à.-d. un porte-documents) et respecter les normes opérationnelles lorsqu'il l'utilise.

10. Les renseignements PROTÉGÉS transmis par voie électronique doivent être chiffrés à l'aide d'un produit conforme à la norme FIPS 140-2.

11. Tous les documents produits ou remplis par l'entrepreneur qui contiennent des renseignements PROTÉGÉS doivent porter la mention affichant la cote de sécurité dans le coin supérieur droit de chaque page. En outre, tout le matériel informatique (p. ex. les ordinateurs, les imprimantes, les supports informatiques amovibles et les bandes de sauvegarde) doit être étiqueté convenablement (marquage de sécurité).

12. Lorsqu'il accède à distance au système informatique, l'entrepreneur devra se connecter à un réseau privé virtuel (RPV) nécessitant une authentification à deux niveaux. Le RPV devra être sécurisé et faire l'objet d'une surveillance visant à prévenir les cyberattaques et l'accès non autorisé aux données. L'employé utilisant le RPV devra être conscient des risques et comprendre les menaces potentielles.

13. Les données contractuelles fédérales devront être conservées séparément des autres données contractuelles et des données d'entreprise, de sorte que l'ensemble des données contractuelles fédérales puisse faire l'objet d'un balayage de sécurité à la demande du client.

14. Tous les disques durs, les supports amovibles, les dispositifs de secours et autres appareils contenant des renseignements PROTÉGÉS devront être détruits conformément aux procédures de sécurité énoncées dans le document ITSG-06 afin de veiller à ce qu'il soit impossible de lire des données PROTÉGÉES résiduelles à partir de ces appareils ou périphériques. Cela inclut également les imprimantes, les imprimantes multifonctions et les photocopieurs qui contiennent un disque dur interne.

15. À moins d'obligations contraires prescrites par la loi, l'entrepreneur doit retirer de façon permanente tout renseignement électronique de nature délicate qui appartient à RHDCC ou qui a été traité dans le cadre du marché de tout dispositif de stockage qui appartient à l'entrepreneur ou à un de ses agents.

16. L'entrepreneur doit veiller à la supervision directe des personnes qui ne détiennent pas de COTE DE FIABILITÉ en vigueur lorsqu'elles procèdent à l'entretien d'un ordinateur utilisé pour traiter des renseignements PROTÉGÉS dans les locaux de l'entrepreneur.

17. S'il faut procéder à l'entretien d'un ordinateur utilisé pour le stockage ou le traitement de renseignements PROTÉGÉS à l'extérieur des locaux de l'entrepreneur, ce dernier devra voir au retrait et à la sécurisation de tout disque dur contenant des renseignements PROTÉGÉS avant que l'ordinateur soit retiré des locaux.

18. S'il a été déterminé que le disque dur de l'ordinateur utilisé pour traiter ou stocker des renseignements PROTÉGÉS n'est plus utilisable, l'entrepreneur doit remettre ce disque dur afin qu'il soit détruit.

19. Toute utilisation d'un réseau sans fil doit être conforme aux lignes directrices sur la configuration énoncées dans le document ITSPSR-21A.

20. L'entrepreneur est responsable de tout dommage résultant de l'atteinte à la sécurité de renseignements PROTÉGÉS.

21. L'entrepreneur doit signaler au chargé de projet toute perte ou tout vol de renseignements PROTÉGÉS dans les deux heures suivant la détection.

22. L'entrepreneur peut demander au chargé de projet un exemplaire de toutes les politiques et les normes ministérielles applicables.