

**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

<b>Title - Sujet</b> VARIABLE DATA - T4 TAX SLIPS	
<b>Solicitation No. - N° de l'invitation</b> G8034-120005/A	<b>Amendment No. - N° modif.</b> 001
<b>Client Reference No. - N° de référence du client</b> G8034-120005	<b>Date</b> 2013-08-09
<b>GETS Reference No. - N° de référence de SEAG</b> PW-\$\$CW-010-63198	
<b>File No. - N° de dossier</b> cw020.G8034-120005	<b>CCC No./N° CCC - FMS No./N° VME</b>
<b>Solicitation Closes - L'invitation prend fin</b> <b>at - à 02:00 PM</b> <b>on - le 2013-08-28</b>	<b>Time Zone</b> <b>Fuseau horaire</b> Eastern Daylight Saving Time EDT
<b>F.O.B. - F.A.B.</b> <b>Plant-Usine:</b> <input type="checkbox"/> <b>Destination:</b> <input type="checkbox"/> <b>Other-Autre:</b> <input type="checkbox"/>	
<b>Address Enquiries to: - Adresser toutes questions à:</b> Werk, Janet	<b>Buyer Id - Id de l'acheteur</b> cw020
<b>Telephone No. - N° de téléphone</b> (613) 998-3968 ( )	<b>FAX No. - N° de FAX</b> ( ) -
<b>Destination - of Goods, Services, and Construction:</b> <b>Destination - des biens, services et construction:</b> see herein	

**Instructions: See Herein**

**Instructions: Voir aux présentes**

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

This amendment is to add the IT security document

All other terms and conditions remain unchanged.

### **IT Security Requirements Technical Document IT Security, Human Resources and Skills Development Canada**

The Human Resources and Skills Development Canada (HRSDC) Security requirements for the above mentioned contract are those included in the Operational Security Standard: Management of Information Technology Security (MITS).

In addition, the following additional requirements are also to be inspected:

1. Each Contractor requiring access to PROTECTED information must hold a valid RELIABILITY STATUS security clearance, granted by the Canadian Industrial Security Directorate (CISD) of Public Works and Government Services Canada (PWGSC).
2. The Contractor shall not provide access to HRSDC information to subcontractors, volunteers, offenders or other parties, unless individuals have been authorized by HRSDC, hold a valid RELIABILITY STATUS clearance and have a legitimate need-to-know for the information provided via that system.
3. The Contractor shall not grant individuals without a RELIABILITY STATUS security clearance access to computers that are or were previously used to process HRSDC information or permit those same individuals to assist with the care or operation of the computer systems used to access HRSDC information.
4. The Contractor shall ensure that all of its employees who are involved in this contract are completely aware of their security obligations related to the handling of PROTECTED information.
5. If PROTECTED information is stored or processed on a computer belonging to the Contractor and/or on removable media such as a USB flash drive, the information must be protected by a strong password and encrypted using a product that meets FIPS 140-2 standard.
6. The Contractor shall operate computers used to complete the contract only in an Operations Zone as defined in the Treasury Board's Operational Security Standard on Physical Security.
7. When not in use, the Contractor(s) must secure all sensitive material stored in removable computer media in a RCMP-approved security container.
8. The Contractor shall ensure that the screen and printed output is not viewable by unauthorized people.
9. The Contractor transporting any PROTECTED information must use a RCMP-approved locking dispatch case (i.e. briefcase) and follow operational standards while handling it.
10. Electronic exchange of PROTECTED information must be encrypted using a product that meets FIPS 140-2 standard.
11. All documentation produced or completed by the Contractor, which contains PROTECTED information shall have its sensitivity labeled in the upper right hand corner on the face of each page of the document. Also all hardware devices (e.g. PCs, printers, removable storage media and backup tapes) will be labelled appropriately. (Security Markings).

12. When using remote access on the Information System (IS) the company shall utilize a VPN solution that requires two tier authentication; is secure and monitored to prevent cyber attacks and unauthorized access. The employee using a VPN must be made aware of the risks and understand the potential threats.

13. Government contractual data is to be segregated from other contractual data and corporate data in a way which allows all government contractual data to be immediately security wiped upon request of the client.

14. All hard disks, removable media, backup media, etc that contain PROTECTED information shall be disposed of using security procedures defined in ITSG-06 to ensure no residual PROTECTED data can be read off these devices, this would also include printers, multi-function printers and photocopiers which utilize an internal hard drive.

15. Unless prescribed otherwise by law, the Contractor must permanently remove all sensitive electronic information that belongs to or was processed in the completion of the contract, from any storage medium belonging to the Contractor or any of its agents.

16. The Contractor shall ensure direct supervision of individuals without a valid RELIABILITY STATUS security clearance if/when they are to service or maintain a computer used to process PROTECTED information on the contractor's premises.

17. If there is a requirement to service a computer that is used to store and/or process PROTECTED information outside of the Contractor's premises, any hard disk(s) containing PROTECTED information must be removed and secured with the Contractor prior to the computer being removed from the premises.

18. If it has been determined that the computer hard disk used to process or store PROTECTED information is no longer serviceable, the Contractor shall surrender the hard disk for destruction.

19. When using wireless, it is to conform to the configuration guidelines in ITSPSR-21A.

20. The Contractor is liable for any damages incurred as a result of the compromise of any PROTECTED information.

21. The Contractor must report to the Project Authority, any loss or theft of PROTECTED information within two hours of detection.

22. The contractor may request a copy of all applicable departmental policies and standards from the project authority.