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

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 Aviation document booklets and labe	
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:**	

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**	

The purpose of this amendment is to respond to make the following revision:

PART 1) In Amendment 008 - PART A -

DELETE Part A in its entirety and REPLACE WITH:

PART A - RESPOND TO BIDDER'S QUESTIONS:

Question 28:

Amendment 002
Annex C - IT Security Requirements Documents – Point 7

Should the reference to "*sensitive*" information be changed to "*Protected*" information?

Response 28:

Annex C - IT Security Requirements Documents – Point 7

The IT security document has been revised. Refer to Part 2 of this amendment.

Question 29:

Amendment 002
Annex C - IT Security Requirements Documents – Point 15

a. This section uses the words "sensitive information" and "agents" which were not previously defined. Should those words be replaced with the word "PROTECTED information" and "subcontractor" respectively?

b. This section requires the Contractor to return or delete all PROTECTED information in its possession at the end of the contract. The Contractor has obligations to maintain records under the SACC Clauses 2030 33 (2014-09-25) Accounts and Audit, and 2030 12 (2014-09-25) Inspection and Acceptance. Can TCCA/PWGSC confirm that the Contractor may maintain PROTECTED B as required under the contract?

Response 29:

Annex C - IT Security Requirements Documents – Point 15

a. The IT security document has been revised. Refer to Part 2 of this amendment.

b. The Contractor must maintain the records as specified in the terms and conditions of the Contract as stated in General Conditions 2030 33 and 2030 12 (2014-09-25) and in accordance with the security requirements of the Contract.

Question 30:

Amendment 002
Annex C - IT Security Requirements Documents – Point 18

This section only refers to Hard drives. Should, similar to Section 15 (previously noted), this reference instead to all storage media (eg: SSDs, DVDs, tapes, USB keys, etc)?

Response 30:

Amendment 002
Annex C - IT Security Requirements Documents – Point 18

The IT security document has been revised. Refer to Part 2 of this amendment.

Question 31:

Amendment 002
Annex C - IT Security Requirements Documents – Point 18

Previous practice, as approved by CISD, is to internally destroy all storage media in accordance with CISD approved practices. Many of a company's devices are used for multiple Government of Canada projects and while the data may be logically separated, it may not be physically separated. Handing over storage media that was used for other GoC contract to TC is problematic. To comply with this requirement a company would likely have to purchase separate servers and other data storage equipment for TC (at a much greater cost to TCCA). Would it be acceptable to follow the practices approved by CISD in the past?

Response 31:
Amendment 002
Annex C - IT Security Requirements Documents – Point 18

The IT security document has been revised. Refer to Part 2 of this amendment.

PART 2) Amendment 002
Annex C - IT Security Requirements Documents

DELETE the *IT Security Requirements Technical Document* , *Aviation Document Booklet (ADB), Transport Canada* **IN ITS ENTIRETY AND REPLACE WITH the following document:**

Security Guide for Contractor Sites, Facilities and Information Technology Equipment Producing, Accessing, Storing and/or Processing Protected B Electronic Information

(the complete document follows this page)

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED

Security Guide for Contractor Sites, Facilities and Information Technology Equipment Producing, Accessing, Storing and/or Processing Protected B Electronic Information

Information Technology Security (ITS) Requirements
(Maximum Sensitivity Protected B)

All TC contractors who use their facilities and/or information technology equipment to access, process and/or store sensitive information rated Protected B are required to agree to the following criteria and to provide the required ITS configuration details of their systems and facilities to Transport Canada IM/IT Security.

Requirements:

1. Must permit security inspection and verification of its information technology infrastructure by Transport Canada (TC) if/when required.

2. Employees of Partners or Third Parties:
   2.1. Employees (including contractors) who are granted access to Protected B information or provide administrative, support or maintenance services for the information technology infrastructure and/or its information assets shall possess a valid minimum enhanced reliability security clearance as per Treasury Board Secretariat (TBS) Personnel Screening Standard.

3. Employ the following administrative controls, concepts and risk management philosophies as identified by TBS Operational Security Standard: Management of Information Technology Security (MITS):
   3.1. Change Management and Control processes for approval of changes to software and hardware;
   3.2. Configuration Management – defined and documented;
   3.3. Keep change log records of maintenance and modification to services and associated systems;
   3.4. Monitoring Protected B systems and alerting TC on the compromise, unauthorized access and/or disclosure of information assets originating from TC.

4. Employ the following technical controls or concepts of operation (where applicable):
   4.1. Access Controls – adequate to prevent unauthorized access. Use defined processes and procedures to grant, revoke and monitor access.
   4.2. Strong Passwords – minimum 8 characters, complexity rules (alpha numeric, special characters, upper and lower case), employ password history, force change at regular intervals and use lockout rules).
   4.3. Role Based Access to information – in support of the concept of “least privilege”
   4.4. Session Termination – provide a reasonable session timeout delay for operating systems and applications.
   4.5. System Use Notification – identify acceptable use and the sensitivity level of information
   4.6. Secure Data Communications – data in transit between various systems and all end-user interfaces such as IPSec, SSL /TLS (Cryptographic products and algorithms must be CSEC approved / NIST-FIPS compliant)
   4.7. Secure Data Storage – data at rest must be encrypted. (Cryptographic products and algorithms must be CSEC approved / NIST- FIPS compliant)
   4.8. Network Segmentation for Protected B servers/databases – employ different network zones to separate workstations/clients, application servers and databases by using firewalls between zones and filtering and restricting traffic/access.
   4.9. Security Infrastructure – employ firewalls, intrusion detection/prevention , malicious code detection between private and public networks (at the border / network perimeter)

4.10. Activity Logging – maintain user access logs and activity logs (unsuccessful login attempts)
4.11. Patch management and Security updates – applied in a timely manner at regular intervals
4.12. Wireless Networking – employ strong authentication and data encryption standards.
4.13. Backup management – backups are encrypted and securely stored.
4.14. Segregation of client data – separation of client data from one client to another;
4.15. Contingency Planning – have reasonable plans for operational recovery

5. Sanitize and dispose of all electronic media which contains or has contained Protected B information according to CSEC and RCMP requirements when hardware is replaced, upgraded, when serviced is discontinued or upon request by Transport Canada.

6. Recommendations and Best Practices:
   6.1. Perform Threat and Risk Assessments (TRA) for applications and IT infrastructure
   6.2. Implement a Network Acceptable Use Policy
   6.3. Establish formal standards and baseline security requirements for approved software and hardware
   6.4. Perform regular Vulnerability Assessments
   6.5. Use two-factor authentication for privileged user / administrator access.
   6.6. Use security best practices when developing custom applications.
   6.7. Apply vendor security best practices when configuring software and hardware
   6.8. Apply the recommendations from NIST SP-800-53 Rev.3