Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

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
Special Projects/Projets Spéciaux
11 Laurier St./11, rue Laurier
Place du Portage/, Phase III
Floor 10C1/Étage 10C1
Gatineau
Québec
K1A 0S5

Title - Sujet GOVT OF CANADA RELOCATION SUPP SVCS	
Solicitation No. - N° de l'invitation M7594-164574/A	**Amendment No. - N° modif.** 008
Client Reference No. - N° de référence du client M7594-164574	**Date** 2016-06-09
GETS Reference No. - N° de référence de SEAG PW-$$ZL-106-30139	
File No. - N° de dossier 106zl.M7594-164574	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2016-06-15**	**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: Sanford, Gordon	**Buyer Id - Id de l'acheteur** 106zl
Telephone No. - N° de téléphone (873) 469-4633 ( )	**FAX No. - N° de FAX** (819) 956-2675
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**	

Canada

Solicitation M7594-164574/A

Amendment 008

This solicitation amendment is raised to:

1. Respond to questions relating to this bid solicitation as detailed in Section A; and
2. Modify the bid solicitation as detailed in Sections B.

SECTION A: QUESTIONS AND ANSWERS

	Question	Answer
Q58	7.6 Security Requirement page 45 – 51. Background: Under the subheading of "Security Requirement for Canadian Supplier," RFP 7.6.5.b states, "[The Contractor/Offeror must comply with the provisions of the] Industrial Security Manual (Latest Edition)." Section 800 of the referenced Industrial Security Manual states that "the security standards contained in the Government Security Policy, Information Technology Standards, are the minimum standards for security in the private sector [emphasis added]." In turn, this reference to the Government Security Policy, Information Technology Standards, links to the Treasury Board Secretariat's "Operational Security Standard: Management of Information Technology Security (MITS)" which provides detailed security requirements in three areas: o Management controls (e.g. security in the System Development Life Cycle, identification and categorization of Information and IT Assets, security risk management, incident management, vulnerability management, continuity planning) o Technical controls (e.g. identification and authentication, authorization and access control, cryptography, public key infrastructure, network and perimeter defence)	Both Canadian and Foreign supplier must abide by the intent of the industrial security manual and abide by the general descriptions of management, technical and procedural security controls identified in the PGS, and MITS. Foreign contractors must also meet the requirements of the industrial security manual, further qualified for foreign suppliers at paragraph 7.6.15. The added information for foreign suppliers is designed by IISD to clarify how a foreign supplier with no direct ability to participate in the industrial security program can demonstrate and effectively meet the intent of the controls.

	o Operational controls (e.g. graduated safeguards, security processes, active defence, detailed prevention, detection, response and recovery controls) MITS contains more than 100 discrete mandatory security requirements (i.e. statements containing "must"). By contrast, under the subheading "Security Requirement for Foreign Supplier," RFP 7.6.15 states "See Appendix B for security measures required for the treatment and access to CANADA PROTECTED information." Appendix B, paragraph 1, states "the following describes the minimum security requirements [emphasis added] for processing, producing and storing CANADA PROTECTED information on information systems." It then lists fewer than 20 controls, several of which appear to be optional, and others that do not reflect current security best practice. Issue: Security requirements will impact bidders' costs to do the following: o Design, engineer, implement, and deploy the solution o Provide secure operations for the service o Manage the service, in particular in the area of continuous risk management The minimum security requirements for Canadian suppliers are substantially greater than those specified for Foreign suppliers, giving Foreign suppliers a financial competitive advantage for their bids. Question: Will Canada ensure a fair competition by providing a common set of technical, operational, and management security requirements for all bidders?	
Q59	7.6 Security Requirement page 45 – 51. Issue: Further to Question #Q58, the current best practice and guidance for the selection, specification, and implementation of security controls for the Government of Canada is	The tailored set of security controls provided in response to this question were derived from: https://www.cse-cst.gc.ca/en/publication/itsg-33 (see ANNEX 4A Profile 1). The specific security controls for Profile 1 that are required to be met by

	provided in the Communications Security Establishment of Canada's ITSG-33 "IT Security Risk Management: A Lifecycle Approach." ITSG-33 provides a process for managing both organizational as well as information systems security in the system lifecycle. ITSG-33 Annex 3 provides a catalog of security controls. To guide the acquisition process, control SA-4 states: (A) "The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable GC legislation and TBS policies, directives and standards, and organizational mission/business needs: (a) Security functional requirements; (b) Security strength requirements; (c) Security assurance requirements; (d) Security-related documentation requirements; (e) Requirements for protecting security-related documentation; (f) Description of the information system development environment and environment in which the system is intended to operate; and (g) Acceptance criteria." The supplemental guidance for control SA-4 states: "Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process." Question: To address a common set of requirements that will apply to both Canadian and Foreign suppliers, will Canada provide the information specified in control SA-4, and provide a tailored set of security controls using the catalog in ITSG-33 Annex 3?	the contractor can be found at the attached Annex E - Contract TBS ITSG-33 Control Requirements. See Section B below for modifications to the bid solicitation.

SECTION B: MODIFICATIONS TO BID SOLICITATION

Modification #31:

At Part 7 – Contract TBS Resulting Contract Clauses, 7.6 Security Requirement add, following Appendix B, "7.6.1 The Contractor must implement the security controls found at the attached Annex E - Contract TBS ITSG-33 Control Requirements."

Modification #32:

At Part 7 – Contract TBS Resulting Contract Clauses, add the attached document, Annex E - Contract TBS ITSG-33 Control Requirements.

Modification #33:

At Contract TBS Annex A Statement of Requirements (SOR), 1.7.1 i., delete "CSEC ISTG guidelines and directives http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti-eng.html)" and replace with:

1. CSE ITSG-33 IT Security Risk Management: A Lifecycle Approach https://www.cse-cst.gc.ca/en/publication/itsg-33
2. CSE ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada https://www.cse-cst.gc.ca/en/node/268/html/15236
3. CSE ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zone https://www.cse-cst.gc.ca/en/node/266/html/25034
4. CSE ITSG-31 User Authentication Guidance for IT Systems https://www.cse-cst.gc.ca/en/node/267/html/22784

Modification #34:

At Contract TBS Annex A Statement of Requirements (SOR), 1.7.1 h., delete "CSEC ITSD guidelines and directives (http://www.cse-cst.gc.ca/its-sti/publications/itsd-dsti-eng.html)" and replace with "ITSD-01a - "Security Directive for the Application of Communications Security Using CSE-Approved Solutions" (https://www.cse-cst.gc.ca/en/node/258/html/15221)".

Modification #35:

At Contract TBS Annex A Statement of Requirements (SOR), 1.7.2 b), delete http://www.tbs-sct.gc.ca/pubs_pol/gospubs/Treasury BoardM_12A/23recon-1_ew.asp and replace with https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328.

Modification #36:

At Contract TBS Annex A Statement of Requirements (SOR), 1.7.1 add:

o. Standard on Web Accessibility - http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

p. Standard on Web Usability - http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227

ALL OTHER TERMS AND CONDITIONS OF THE BID SOLICITATION REMAIN UNCHANGED

Annex E – Contract TBS ITSG-33 Control Requirements			
Family	**Control ID**	**Enhancement**	**Name**
AC	1		ACCESS CONTROL POLICY AND PROCEDURES
AC	2		ACCOUNT MANAGEMENT
AC	3		ACCESS ENFORCEMENT
AC	3	(7)	ACCESS ENFORCEMENT
AC	3	(9)	ACCESS ENFORCEMENT
AC	3	(10)	ACCESS ENFORCEMENT
AC	4		INFORMATION FLOW ENFORCEMENT
AC	5		SEPARATION OF DUTIES
AC	6		LEAST PRIVILEGE
AC	6	(5)	LEAST PRIVILEGE
AC	6	(9)	LEAST PRIVILEGE
AC	6	(10)	LEAST PRIVILEGE
AC	7		UNSUCCESSFUL LOGIN ATTEMPTS
AC	8		SYSTEM USE NOTIFICATION
AC	17		REMOTE ACCESS
AC	18		WIRELESS ACCESS
AC	19		ACCESS CONTROL FOR MOBILE DEVICES
AC	19	(100)	ACCESS CONTROL FOR MOBILE DEVICES
AC	22		PUBLICLY ACCESSIBLE CONTENT
AT	1		SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT	2		SECURITY AWARENESS
AT	2	(2)	SECURITY AWARENESS
AT	3		ROLE BASED SECURITY TRAINING
AU	1		AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU	2		AUDITABLE EVENTS
AU	3		CONTENT OF AUDIT RECORDS
AU	4		AUDIT STORAGE CAPACITY
AU	4	(1)	AUDIT STORAGE CAPACITY
AU	6		AUDIT REVIEW, ANALYSIS, AND REPORTING
AU	8		TIME STAMPS
AU	12		AUDIT GENERATION
CA	1		SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES
CA	3		INFORMATION SYSTEM CONNECTIONS
CA	3	(3)	INFORMATION SYSTEM CONNECTIONS
CA	6		SECURITY AUTHORIZATION

CM	1		CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
CM	2		BASELINE CONFIGURATION
CM	3		CONFIGURATION CHANGE CONTROL
CM	5		ACCESS RESTRICTIONS FOR CHANGE
CM	6		CONFIGURATION SETTINGS
CM	7		LEAST FUNCTIONALITY
CM	7	(5)	LEAST FUNCTIONALITY
CM	8		INFORMATION SYSTEM COMPONENT INVENTORY
CM	9		CONFIGURATION MANAGEMENT PLAN
CP	1		CONTINGENCY PLANNING POLICY AND PROCEDURES
CP	9		INFORMATION SYSTEM BACKUP
IA	1		IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
IA	2		IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA	3		DEVICE IDENTIFICATION AND AUTHENTICATION
IA	4		IDENTIFIER MANAGEMENT
IA	5		AUTHENTICATOR MANAGEMENT
IA	5	(1)	AUTHENTICATOR MANAGEMENT
IA	5	(9)	AUTHENTICATOR MANAGEMENT
IA	6		AUTHENTICATOR FEEDBACK
IR	1		INCIDENT RESPONSE POLICY AND PROCEDURES
IR	9		INFORMATION SPILLAGE RESPONSE
MA	1		SYSTEM MAINTENANCE POLICY AND PROCEDURES
MP	1		MEDIA PROTECTION POLICY AND PROCEDURES
MP	2		MEDIA ACCESS
MP	3		MEDIA MARKING
MP	4		MEDIA STORAGE
MP	5		MEDIA TRANSPORT
MP	8		MEDIA DOWNGRADING
MP	8	(3)	MEDIA DOWNGRADING
PE	1		PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PE	2		PHYSICAL ACCESS AUTHORIZATIONS
PE	2	(100)	PHYSICAL ACCESS AUTHORIZATIONS
PE	3		PHYSICAL ACCESS CONTROL
PE	4		ACCESS CONTROL FOR TRANSMISSION MEDIUM
PE	6		MONITORING PHYSICAL ACCESS
PE	6	(4)	MONITORING PHYSICAL ACCESS
PE	8		ACCESS RECORDS

PE	16		DELIVERY AND REMOVAL
PE	18		LOCATION OF INFORMATION SYSTEM COMPONENTS
PE	18	(1)	LOCATION OF INFORMATION SYSTEM COMPONENTS
PL	1		SECURITY PLANNING POLICY AND PROCEDURES
PL	2		SYSTEM SECURITY PLAN
PL	4		RULES OF BEHAVIOUR
PL	7		SECURITY CONCEPTS OF OPERATION
PL	8		INFORMATION SECURITY ARCHITECTURE
PL	8	(1)	INFORMATION SECURITY ARCHITECTURE
PL	8	(2)	INFORMATION SECURITY ARCHITECTURE
PS	1		PERSONNEL SECURITY POLICY AND PROCEDURES
PS	3		PERSONNEL SCREENING
PS	4		PERSONNEL TERMINATION
PS	5		PERSONNEL TRANSFER
PS	6		ACCESS AGREEMENTS
PS	7		THIRD-PARTY PERSONNEL SECURITY
RA	1		RISK ASSESSMENT POLICY AND PROCEDURES
RA	2		SECURITY CATEGORIZATION
RA	3		RISK ASSESSMENT
SA	1		SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
SA	9		EXTERNAL INFORMATION SYSTEM SERVICES
SA	18		TAMPER RESISTANCE AND DETECTION
SC	1		SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC	2		APPLICATION PARTITIONING
SC	5		DENIAL OF SERVICE PROTECTION
SC	7		BOUNDARY PROTECTION
SC	7	(3)	BOUNDARY PROTECTION
SC	7	(5)	BOUNDARY PROTECTION
SC	7	(9)	BOUNDARY PROTECTION
SC	8		TRANSMISSION CONFIDENTIALITY AND INTEGRITY
SC	18		MOBILE CODE
SC	23		SESSION AUTHENTICITY
SC	24		FAIL IN KNOWN STATE
SC	28		PROTECTION OF INFORMATION AT REST
SI	1		SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SI	2		FLAW REMEDIATION
SI	3		MALICIOUS CODE PROTECTION

SI	4		INFORMATION SYSTEM MONITORING
SI	5		SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
SI	8		SPAM PROTECTION