



RETURN BIDS TO:

RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions -
TPSGC

11 Laurier/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
Parliamentary Precinct Division/Acquisitions de la Cité
parlementaire
222 Queen Street / 222, rue Queen
Ottawa
Ontario
K1A 0S5

Title - Sujet Invitation to Qualify (ITQ) Modern Log and Event Management (MLEM) Solution	
Solicitation No. - N° de l'invitation EP750-220056/A	Amendment No. - N° modif. 003
Client Reference No. - N° de référence du client EP750-220056	Date 2022-09-28
GETS Reference No. - N° de référence de SEAG PW-\$PPS-002-28784	
File No. - N° de dossier 002pps.EP750-220056	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM Eastern Daylight Saving Time EDT on - le 2022-10-11 Heure Avancée de l'Est HAE	
F.O.B. - F.A.B.	
Plant-Usine: <input type="checkbox"/> Destination: <input checked="" type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Sobnath, Keshav	Buyer Id - Id de l'acheteur 002pps
Telephone No. - N° de téléphone (343) 576-2756 ()	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

Amendment No. 003 is raised to extend the closing date of Solicitation number: EP750-220056/A, address the changes herein and address questions received in QUESTION AND ANSWER SERIES 3.

- A) Extend the closing date of the Solicitation number: EP750-220056/A from “Monday October 3, 2022 at 14:00 EDT” to “Tuesday October 11, 2022 at 14:00 EDT”**
- B) Include the following attachments as part of the Invitation to Qualify (ITQ):**
 - i. ANNEX F INITIAL INTERNATIONAL SECURITY SCREENING (IISS) FORM**
 - ii. ANNEXE F FORMULAIRE DE FILTRAGE INITIAL DE SÉCURITÉ INTERNATIONALE**
- C) DELETE section “5.2.3 Security Requirement – Required Documentation” in its entirety and REPLACE with the following:**

“5.2.3 Security Requirement – Required Documentation

In accordance with the requirements of the Contract Security Program of Public Works and Government Services Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html>), the Respondent must provide a completed Contract Security Program Application for Registration (AFR) form **and/or** Initial International Security Screening (IISS) form to be given further consideration before the Phase 2 – Request for Proposal (RFP).

Respondents are reminded to obtain the required security clearance and, as applicable, security capabilities promptly. As indicated above, respondents who do not provide all the required information at ITQ closing date, they will be given the opportunity to complete any missing information from the AFR form and/or IISS form within a period set by the Contracting Authority. If that information is not provided within the timeframe established by the Contracting Authority (including any extension granted by the Contracting Authority in its discretion), or if Canada requires further information from the Respondent in connection with assessing the request for security clearance (i.e., information not required by the AFR form and/or IISS form), the Respondent will be required to submit that information within the time period established by the Contracting Authority, which will not be less than 48 hours. If, at any time, the Respondent fails to provide the required information within the timeframe established by the Contracting Authority, its response will be declared non-responsive.”

D) Address the questions received.

QUESTION AND ANSWER SERIES 3:

Q1. Question regarding requirements 4.1 & 4.2, which seem to be mutually exclusive.

E4. Solution delivery			
E4.1	On-premise COTS solution	Mandatory	The solution must have the ability to deliver the required capabilities using components deployed solely on-premise.
E4.2	Cloud-based solution	Mandatory	The solution must have the ability to deliver the required capabilities using components deployed solely in the cloud (SaaS, PaaS).

E4.1 & E4.2 states that the solution must be able to be delivered solely on-premise and able to be solely delivered in the cloud. This seems to be a statement that cannot be satisfied, as the two components to it are mutually exclusive.

A1. The solution must support the ability to be deployed exclusively on-premises or exclusively deployed in the cloud, the solution must be able to support both deployment models.

----- | -----

Q2. As it relates to Section 5.2.3 of the ITQ document, is the requirement to provide a completed Contract Security Program Application for Registration (AFR) form only applicable to Respondents who are not currently registered with the Contract Security Program? Can Respondents who are already registered and have obtained an organization clearance provide this information without having to resubmit the application form?

A2. Please refer to part C) of this document (Amendment No. 003). As per Section 5.2.3 Security Requirement – Required Documentation, **ALL** respondents must provide must provide a completed Contract Security Program Application for Registration (AFR) form **and/or** Initial International Security Screening (IISS) form to be given further consideration.

----- | -----

Q3. As it relates to Mandatory Requirement number E4.1, could Canada specify what capabilities need to be deployed on-premises? As drafted, the requirement seems too broad as it would apply to the entire solution. "Would Canada consider that key log and event capture and processing components be on premises, with storage and additional processing in the cloud?"

A3. As related to Mandatory Requirement number E4.1, all capabilities of the solution must support a deployment exclusively on-premises.

----- | -----

Q4. According to the SRCL (Part A - Sect 6(b)), the Supplier will require access to restricted access areas, but will not have access to Protected information. Could Canada please confirm that the Supplier will not have access to Protected information and that clearance will only be required for personnel providing services on-site?

A4. Yes, confirmed.

----- | -----

Q5. ANNEX B: EVALUATION CRITERIA SPREADSHEET

- i. I'm not sure what a submission should look like. There are four specific items identified in the spreadsheet that suggests that we would run the cloud deployment.
 - 1. Our architecture is designed to run as easily in the cloud as it runs on-premise. However, the users run the deployment in the cloud and can host in any data center they choose. For example, one of criteria suggest that the data must reside and be hosted in Canada. Our architecture allows the end user to keep the data wherever they want. We do not target any cloud vendor.
 - 2. Another criteria is Cloud Security certifications. Once again, we do not host the deployment or the data, so it's up the end user to choose the hosting vendor, and decide which security certifications are relevant to them.
- ii. Data Retention capabilities: That would be up to the end user to decide on data retention. As a native hybrid solution, our SaaS solution can be set up to access any data source, and retention of that source would be decided the by end user, rather than by our solution.

A5. For the Cloud-based solution, we expect a fully managed SaaS solution that can be deployed in a cloud service provider that meets our mandatory hosting, data residency and security certification requirements.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME