



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

Quebec

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

Systems Software Procurement Division / Division des
achats des logiciels d'exploitation
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

Title - Sujet Proactive Monitoring	
Solicitation No. - N° de l'invitation B7310-190250/A	Amendment No. - N° modif. 005
Client Reference No. - N° de référence du client B7310-190250	Date 2019-07-11
GETS Reference No. - N° de référence de SEAG PW-\$\$EE-063-35752	
File No. - N° de dossier 063ee.B7310-190250	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2019-07-26	Time Zone Fuseau horaire Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Smallwood, Jeffrey	Buyer Id - Id de l'acheteur 063ee
Telephone No. - N° de téléphone (613) 794-0826 ()	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

=====

Question:

Would you mind to share with me what's the approximate budget.

Response:

The budget has not yet been determined

=====

Question:

Could you check if my company is eligible to bid for this project.

Response:

All companies are invited to provide a proposal.

=====

Question:

For this current request, is the Crown able to confirm if this RFP was a result of a previous RFI? IF yes, could you please share the RFI reference number?

Response:

The Crown can confirm that this RFP was not the result of an RFI.

=====

Question:

Is this RFP a result of a previous Proof of Concept?

Response:

This RFP is not the result of a previous Proof of Concept.

=====

Question:

Has there currently been any previous questions / answers issued on this RFP?

Response:

Yes, previous questions were posed / answered on this RFP

=====

Question:

With regards to the new SSC Cyber Security Procurement Vehicle that has started qualifying vendors, has the Crown considered procuring this desired solution through the CSPV?

Response:

The Crown did not consider procuring the solution through the CSPV.

=====

Question:

Is there an existing network management / monitoring tool that would be required to be integrated into this requested solution?

Response:

There currently is not an existing network management / monitoring tool that would be required to be integrated into this requested solution.

=====

Question:

In our efforts to ensure accurate scoping of the solution, could the Crown please provide an estimation of the logs volume of the in-scope devices that will be part of the integrated solution and a list of those in-scope devices (log sources) with any version details that can be provided? This would also include expected log volume of the in-scope application(s), operating systems and network components. The following would also be helpful:

- GB/Day for in-scope logs
- Events per second for in-scope logs
- Average event size for each data source

Response

At this time, the best that the Crown can provide at this point is a +/-50% ball park estimate:

1. Production Servers – 10 Millions entries @ +/-50%
2. Staging Servers – 5 Millions entries @ +/-50%

To produce something more accurate, the Crown would need additional lead time and specific details of the required / requested logs (i.e.: Audit logs, Security logs, Application logs, System logs, etc.)

=====

Question:

Could the Crown please confirm the required on-line and long-term retention period of data/logs for this solution?

Response

As per CM.01 The EM Solution must be able to keep a record of all captured Authorized Users' actions of suspected cases of information malfeasance and misuse over a user configurable time period of at least 5 years.

=====

Question:

The industry method for employee monitoring via UBA/UEBA technologies has shifted from the traditional SIEM rule/use-case with correlation to leverage modeling and machine learning. To reflect this, we would like to request that language be added to References in Attachment 1 - Functional and Non-Functional Requirements. Where the requirement states "via rules/uses-cases/correlation", we would request that the language be amended to "via rules/uses-cases/correlation OR via the use of modeling and machine learning". Could the Crown please confirm if this would be acceptable?

Response

No, the suggested amendment is not acceptable.

=====

Question:

The demo scenarios in Attachment 3 - EM Solution Use Case and Demonstration Scenarios, are currently focused on rule creation, use-case creation and correlation of events triggered by those rules and use-cases. For solutions that are leveraging modeling and machine learning, we would be unable to demo any of these scenarios as written as we would require modeling. The benefit of solutions that are leveraging AI, ML and modeling, is that you will greatly reduce the ongoing management effort as you shift from having to design rules based on what threats might occur or what you might consider malicious activities by employees to a solution where ML and modeling allows for the focus to be shifted to a what is normal and what isn't model. To demo solutions that are leveraging AI, ML and modeling, we ask that recorded demos and demos of existing demo environments be allowed to demonstrate the scenarios. We also ask that modeling be accepted versus traditional rule based triggered events. The use of ML for future solutions is one of the digital strategy recommendations from TBS and thus, we would like to present a solution to IRCC that matches this strategy. Could the Crown please confirm if this type of demo would be acceptable?

Response

The bidder is not permitted to use a recorded demo. The bidder is permitted to use an existing environment to demonstrate the scenarios as long as the environment is representative of an enterprise case management system such as GCMS. IRCC requires the bidders to demonstrate rule based triggered events as per Attachment 3 – EM Solution Use Case and Demonstration Scenarios and Employee Monitoring Evaluation Criteria – Product Demonstration.

=====

Question:

From a scoring perspective in Attachment 1, we are requesting that points be awarded in the case where bidders can demonstrate that a requirement is met within a schedule roadmap release, as long as it is prior to the go-live date of the IRCC solution. Could the Crown please confirm if this is acceptable?

Response

For evaluation purposes, requirements that can be demonstrably met by product enhancements contained in scheduled release prior to go-live but are not available at time of bid closing will be considered as customization and will be scored accordingly.

=====

Question:

For requirement DR.E01, the typical solution for this, is to have these events/logs be sent to an external source. We are asking that the wording of this requirement be modified to include "or that these activity logs have the ability to be sent to an external source/location in real-time as the activities occur". Could the Crown please confirm if this is acceptable?

Response

Please clarify what external source/location you are proposing to export to?

=====

Question:

For requirement DR.F04, many of the vendors in this particular technology vertical are just developing their footprint globally and therefore have focused strictly on English as the interface language. We are asking that points be awarded if the vendor commits to adding French as an option prior to a specific date via scheduled roadmap. Could the Crown please confirm if this is acceptable?

Response

For evaluation purposes, requirements that can be demonstrably met by product enhancements contained in scheduled release prior to go-live but are not available at time of bid closing will be considered as customization and will be scored accordingly.

=====

Question:

For requirement DR.F11, could the Crown please define what would be considered a multiple tenant solution in this case?

Response

Tenants are defined as separately managed network/directory domains using different policy sets.