**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**<br>Proactive Monitoring | |
| **Solicitation No. - N° de l'invitation**<br>B7310-190250/A | **Amendment No. - N° modif.**<br>002 |
| **Client Reference No. - N° de référence du client**<br>B7310-190250 | **Date**<br>2019-07-04 |
| **GETS Reference No. - N° de référence de SEAG**<br>PW-$$EE-063-35752 | |
| **File No. - N° de dossier**<br>063ee.B7310-190250 | **CCC No./N° CCC - FMS No./N° VME** |
| **Solicitation Closes - L'invitation prend fin**<br>**at - à 02:00 PM**<br>**on - le 2019-07-09** | **Time Zone**<br>**Fuseau horaire**<br>Eastern Daylight Saving Time EDT |
| **F.O.B. - F.A.B.**<br>**Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐ | |
| **Address Enquiries to: - Adresser toutes questions à:**<br>Smallwood, Jeffrey | **Buyer Id - Id de l'acheteur**<br>063ee |
| **Telephone No. - N° de téléphone**<br>(613) 794-0826 ( ) | **FAX No. - N° de FAX**<br>( ) - |
| **Destination - of Goods, Services, and Construction:**<br>**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**<br>**Raison sociale et adresse du fournisseur/de l'entrepreneur**<br><br>**Telephone No. - N° de téléphone**<br>**Facsimile No. - N° de télécopieur** | |
| **Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)**<br>**Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)**<br><br>**Signature** **Date** | |

Please note: the closing date for this solicitation is being extended to 26th July 1400 hours EST

This question was posed by a potential bidder:

Question #1
The phone number is the solicitation is not active. Would you be able to provide an updated number?

Response to question #1
The correct phone number for Jeff Smallwood is 613-794-0826

==========

Question #2
After reviewing the RFP for Proactive Monitoring on Buy and Sell, Company name believes that we could provide a compliant and value-added solution. We would like to request a one-week extension to the closing date of the solicitation to ensure enough time to put together a detailed response with all requirements being demonstrated fully. Would the Crown accept an extension to the closing date to July 16, 2019?

Response to question #2
See above
==========

**Reference:** Statement of Work, Annex B – Volumetrics
**Question 3:**
IRCC has provided some volumetric data for their GCMS environment. The solution we are proposing is not licensed per user, nor per # of servers. Instead we license based on volume of data(logs) ingested on a daily basis. Can IRCC please provide some ballpark estimates on the volume of logs being generated daily by the systems?

Response to question #3

IRCC does not currently maintain these types of volumetrics. The Bidder should use its own volumetric estimates based upon the numbers of users and types of applications provided in the RFP.

==========

**Reference**: Evaluation Criteria – Product Demonstration Document, Section 1, sub-section 3 - Monitor a sub set of System of Record files
**Question 4:**
IRCC has asked for a nested rule to be applied to monitor Authorized users accessing a sub set of System of Record case files. Is IRCC providing a static list of what data individual users or roles can access? Has the system already flagged which data is considered sensitive?

Response to question #4

For the purpose of the demonstration, IRCC does not expect the bidders to use IRCC data. The bidders should use their own data set, but it is recommended that the data be reflective of an enterprise case management system. In the implementation phase IRCC will provide a static list of what data individual users or roles can access and data that is considered sensitive.

==========

**Reference:** Evaluation Criteria – Product Demonstration Document, Section 1, sub-section 3 - Monitor a sub set of System of Record files

**Question 5:**

IRCC has asked for a nested rule to be applied to monitor authorized users taking a screenshot of the System of Record. Can IRCC please expand on this requirement? Does IRCC have existing endpoint software that monitors for this occurrence? Does the action of users taking a screenshot get logged anywhere on the system? Is IRCC expecting the EM solution to perform that function? We are trying to understand the use case driving this requirement (e.g. what's stopping an authorized user from using his smartphone to take a picture of the screen?)

Response to question #5

IRCC does not currently have software that monitors for screen shots. Taking a print-screen has been identified as behaviour indicative of misuse or malfeasance. IRCC would like the EM solution to be able to identify when an authorized user has taken a screen shot.

==========

**Reference**: General

**Question 6:** Are all GCMS application logs currently consolidated centrally (e.g. database or central logging solution)? Could IRCC describe the format of the application logs? Would it be possible to share an existing application log?

Response to question #6

Format of logs would be screenshots and user-interface logs, such as user commands, mouse clicks, etc. The department does not have examples since it does not have an existing EM installed.

==========

**Reference**: Evaluation Criteria – Product Demonstration Document, Section 1, sub-section 2 - Generate an alert when multiple business rules are triggered

**Question 7:**

IRCC has asked for a nested rule to be applied to monitor authorized users accessing the system outside of expected business hours. Are these static values that IRCC is looking to input into the EM solution or is IRCC looking for the solution to identify, based on history and via applied machine learning algorithms, what the expected business hours of each user should be?

Response to question #7

The expected business hours are defined in the system of record (GCMS) based on user's profile, which includes the office where they work.

==========

**Reference**: General
**Question 8**: Can IRCC provide metrics around how many investigations they currently (or plan to) perform on a weekly basis?

Response to question #8

We cannot quantify volumes given that the monitoring tool is not yet in place. Hence, we have no benchmark to provide such information.

==========

**Reference**: Attachment 1 – Functional and Non-Functional Requirements, Monitor Detect Alert section – AR.B07
**Question 9**: IRCC has stated "When an End-Point agent is installed, the EM Product should be able to capture session recordings of user activities for Authorized Users". Can IRCC please clarify what is meant by "End-Point agent". Is IRCC referencing an existing session recording solution that has an End-Point agent? Our solution is capable of ingesting data from any 3rd party session recording solution (e.g. CyberArk, Centrify, etc) but are unclear based on the written requirement if IRCC expects the EM solution to provide the session recording capability.

Response to question #9

IRCC does not have an existing session recording solution. The reference to "End-Point agent" is if the bidder's solution works from a client running on an end-point. Requirement AM.C01 describes the expectation of the solution for capturing authorized user actions.

==========

Question 10
**In the 'Attachment 1 - Functional and Non-Functional Requirements - May 2, 2019.xlsx', under 'DM.F03', it states, "The EM Product must have the ability to monitor, detect, and alert for suspected cases of information malfeasance and misuse without the use of an end-point agent or the need to have anything installed on end-point devices."**

Is this a mandatory requirement? i.e. the monitoring agent cannot be installed on the user/end-point device? If so, do you need it installed on a server?

Response to question #10

Response: Yes, this is a mandatory requirement. The EM Solution must be able to monitor, detect and alert without the use of end-point agents. There is a rated requirement (req AR.B07) for additional functionality that can be provided through the use of an end-point agent.

==========

**Question 11**
**On the same document, under 'DM.F04' it states, "RedHat Enterprise Linux 6 and higher" needs to be supported.**

Is this a mandatory requirement?

Response to question #11
Response: The question references the following mandatory requirement (DM.F04):

The EM Product must support running in the following Operating System environment:

1. Microsoft Server 2012 64 bit and higher; and
2. RedHat Enterprise Linux 6 and higher

The product must support running in one OR the other, not AND.