Service | Innovation | Value

SHARED SERVICES CANADA

Request for Information for the Procurement Process for Enterprise Monitoring Solution (EMS)

Request for Information No.	[RFI No.]	Date	[Date of Release]
GCDocs File No.	[GC Docs File No.]	GETS Reference No.	[GETS Reference No.]

Issuing Office	Shared Services Canada 180 Kent Street, 13th Floor Ottawa, Ontario K1P 0B5	
Contracting Authority (The Contracting Authority is SSC's representative for all questions and comments about this document.)	Name	Guylaine Dagenais
	Telephone No.	343-542-2341
	Email Address	guylaine.dagenais@canada.ca
	Postal Address	180 Kent St, 13 Floor PO Box/CP 9808 STS T CSC, Ottawa, Ontario K1G 4A8
Closing Date and Time	October 4, 2019	
Time Zone	Eastern Daylight Time (EDT)	
Destination of Goods/Services	Not applicable – Request for Information Only	
Email Address for Submitting your Response by the Closing Date	guylaine.dagenais@canada.ca	

SHARED SERVICES CANADA

Request for Information
for the Procurement Process for
Enterprise Monitoring Solution (EMS)

TABLE OF CONTENTS

SHARED SERVICES CANADA

Request for Information for the Procurement Process for Enterprise Monitoring Solution (EMS)

1. General Information

1.1 Introduction

a) **Phase 1 of Procurement Process**: This Request for Information (RFI) is the first phase of a procurement process by Shared Services Canada (SSC) for Enterprise Monitoring Solution (EMS) (the "**Project**"). Suppliers are invited to submit responses to assist Canada in refining its requirements for the Project. Suppliers are not required to submit a response to this RFI in order to participate in any later phases of the procurement process for the Project.

b) **RFI Phase is not a Bid Solicitation**: This RFI is not a solicitation of bids or tenders. No contract will be awarded as a result of the activities undertaken during this RFI. Canada reserves the right to cancel any of the preliminary requirements described as part of the Project at any time during the RFI or any other phase of the procurement process. Given that the RFI process and any related procurement activity may be partially or completely cancelled by Canada, it may not result in any subsequent procurement processes.

c) **Response Costs**: SSC will not reimburse any supplier or any of its representatives for any overhead or expenses incurred in participating in or responding to any part of the RFI phase. Suppliers are also responsible for carrying out their own independent research, due diligence and investigations (including seeking independent advice) that they consider necessary or advisable in connection with their participation in the RFI process and any future procurement process.

1.2 Overview of the Project

a) **Overview of Project**:

The Government of Canada (GC) is exploring modernizing the way monitoring is performed for infrastructure and applications with the following goals:

1) Improving our ability of the returning service;
2) Help drive more valued work from our support organization by reducing mundane tasks;
3) Reduce blind spots by providing a centralized view for monitoring all infrastructure and in-scope applications;
4) Transform the monitoring capability from a re-active to a proactive.

Shared Services Canada (SSC) understands that there is no one tool that can perform all functions required. SSC has a preference to acquire this capability from a Software as a Service (SaaS) perspective but may need to deploy an in-house solution due to security requirements. The tool(s) must interface to the SSC IT Service Management (ITSM) tool as the system of record for events, and actions taken by the provided tool(s).

Currently the GC operates networks with different security designations. For the purpose of this RFI, you should assume we have three networks in scope (unclassified, Secret &

Protected-B) (https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.

SSC sees monitoring broken down into four areas:

1) Availability – is the component operational or not;
2) Performance – is the component performing as expected;
3) Remediation – Automatic execution of a workflow based on an event;
4) Prediction – Transform us from a re-active to a pro-active monitoring posture.

Stakeholders

The primary users of the solution will include Data Centre Services Branch (DCSB), Networks, Security and Digital Services (NSDS), and Service Delivery and Management Branch (SDMB) - Enterprise Command Centre (ECC).

Business Requirements

This RFI seeks information in relation to:

1) Predictive capability using Artificial Intelligence (AI) for IT operations;
2) Availability of the applications, and infrastructure by using Event Management;
3) Auto remediation (robotic automation) to improve our ability to speed up the return to service;
4) Application Performance Monitoring for applications in legacy, and enterprise data centres that service internal Government personnel and citizens.

Constraints

Each network will need to conform to Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38) & Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22). The expectation, is the solution will require hub/relay management servers, deployed in each zone.

The solution must comply with ITSG-33 IT Security Risk Management: A Lifecycle Approach security controls.

The monitoring solution is a critical IT application, and will require being highly available and deployed, within multiple sites to survive a site failure.

In addition, the expectation is that the ITSM tool used at SSC will be the system of record for any detected event and remediation action.

Availability

The Enterprise Command Centre (ECC) will be the focal point to receive all alerts. The ECC is located in multiple facilities, and monitoring alerts are routed to specific teams. The GC has a large investment in monitoring tools, and does not expect to replace them quickly with a new set of tools. A hybrid model of new agent/agentless monitoring to the endpoint as well as routing our main consoles to the new solution, is envisioned.

Performance

SSC clients are requesting application performance monitoring (APM) as a service from SSC to monitor business applications. To accomplish this, SSC needs to capture performance counters of infrastructure as well as application metrics. SSC is continuing its workload migration activities, and application are being migrated to enterprise data centres, following a multi-year plan. SSC believes we require a mix of APM tools to support both legacy as well as enterprise data centres.

Robotic Automation

Within SSC, support activities to some partners are still being performed, as was required before SSC's creation. Various teams of Subject Matter Experts (SME's) have developed scripts to automate tasks, while others follow a traditional manual approach. SSC would like to improve our time to return to service, and increase our quality of execution by using automation technology. SSC sees implementing this technology, will allow our SME's more time to focus on innovation, and value add work to our partners. This automation technology must interface to our ITSM tool as our system of record. This automation technology must not only support our compute platforms, but also include network, storage, and application parameter settings.

Proactive Solution

The technology that SSC manages is evolving from traditional compute/network/storage to cloud, micro services, and the Internet of Things (IoT). With the deluge of structured, and unstructured data, machine-learning technology, will allow for the aggregation of data, and will yield in improvements of availability/performance. The use of analytics, and Machine Learning (ML) will provide in real-time to SSC a view of the state of the supported environment. We see this technology having the ability to understand the business cycle, and evolve the monitoring from traditional reacting to telemetry values to establishing dynamic baselines. The root cause analysis knowledge base, will shift from documents in disparate repositories, to being integrated into this solution, allowing the technology to aid in the decision making process.

Monitoring Tool Interface

Authorized clients shall have the ability via a portal to alter the monitoring rules for their infrastructure and applications. The solution must be capable of operating in both official languages (English & French), and pick up the language settings from the user's desktop. The viewing of the data must be represented in a situational awareness dashboard that requires no coding. The dashboard must operate in real-time, and accept feeds from event management, AI/ML, system logs, and application performance tools. The solution shall take the telemetry from the various sources and produce shapes that can be organized as defined by the stakeholder.

The solution needs to integrate with active directory for user/administrator authentication.

ITSM Tool Integration

SSC has awarded a contract for a new ITSM tool and the monitoring solution will need to interface with this tool:

1) The ITSM tool will be the system of record for all incidents;
2) Event management will enrich the event data by querying the Configuration Management Data Base (CMDB) within the ITSM tool.

Assumptions

The vendor should assume SSC has:

1) Redundant wide area network is in place to the provider, and redundant connections to each location running servers.

b) **Scope of Anticipated Procurement:**

i) **Potential Client Users**: This RFI is being issued by SSC. It is intended that the contract(s) resulting from any subsequent solicitation would be used by SSC to provide shared services to one or more of its clients. SSC's clients include SSC itself, those government institutions for which SSC's services are mandatory at any point during the life of any resulting instrument(s), and those other organizations for which SSC's services are optional at any point during the life of any resulting instrument(s) and that choose to use those services from time to time. Any subsequent procurement process will not preclude SSC from using another method of supply for any of its clients with the same or similar needs, unless a subsequent solicitation for this Project expressly indicates otherwise.

ii) **Number of Contract(s)**: Canada is currently contemplating the award of one contract.

iii) **Term of any Resulting Contract(s)**: Canada is currently contemplating a contract period of 7 years, plus 2 option periods of 2 year each.

c) **National Security Exemption:** This requirement is exempt from trade agreements as the National Security Exemption (NSE) has been invoked.

d) **Preference for Canadian Goods and Services**: The requirement may be subject to a preference for Canadian goods and/or services. This will be set out in any subsequent solicitation.

1.3 Volumetric or Historical Data

The following sample inventory data has been provided to suppliers to assist them in understanding Canada's requirements. The inclusion of this data in this RFI does not represent a commitment by Canada that Canada's future usage or purchase of licenses will be consistent with this data. It is provided purely for information purposes. Although it represents the best information currently available to SSC, Canada does not guarantee that the data is complete or free from error.

Category	# Units	Description
Wifi	80,000	Access points
	16,000	WIDS
Network	19,000	Access switches
	6,000	Edge switches
	4,000	Routers
	75	Optical equipment (SMS)
Data Centres	5,000	Firewalls/Nexus, HIDS/NIDS/TAPS
	50,000	Virtual servers (Linux/Unix/Windows)

Category	# Units	Description
	3,000	Physical servers (Linux/Unix/Windows, High Performance Compute)
Storage	1,000	SAN, NAS, Tape devices
Storage	30	Petabytes
Mainframe	25	Approx. 10 LPAR per mainframe
	1,000	Mainframe applications
Buildings	102	Enterprise & legacy data centres
	1,800	(racks, card access, HVAC, power, cameras)
Applications	20,000	Applications varying from home-grown, open source, SAP, Peoplesoft etc.
Databases	5,000	MS SQL, Oracle, DB2, Sybase
Web Instances	7,500	IIS, Apache, WAS
Cloud	3	Public cloud
Cloud	2	Private cloud

Major Tools Used at SSC

- CA UIM/APM/Spectrum
- IBM Tivoli
- WhatsUp Gold
- HP SIM
- SolarWinds
- MS SCOM
- Nagios
- BMC Patrol

1.4 Submitting Questions

a) Questions about this RFI can be submitted to the Contracting Authority at his or her email address identified on the cover page up until 5 working days before the closing date and time indicated on the cover page of this document. Canada may not answer questions received after that time.

b) To ensure the consistency and quality of information provided to suppliers, significant questions received and the answers will be posted on the Government Electronic Tendering Service (GETS) as an amendment to this RFI.

2. Information Requested by Canada

2.1 Comments on Preliminary Documents

All documents reflecting Canada’s anticipated requirements for this Project that are provided to suppliers during the RFI process are preliminary or draft requirements only and are subject to change. These requirements, or parts of them, may be updated before or during any subsequent solicitation.

Suppliers are requested to provide their comments, concerns and, where applicable, alternative suggestions regarding how the requirements or objectives described for the Project could be satisfied. Suppliers are also invited to provide comments regarding the content, format and/or organization of any draft documents provided with this RFI. Suppliers should explain any assumptions they make in their responses.

2.2 Responses to Questions for Industry

Canada requests responses to the following questions:

a) To minimize the sprawl of hub/relay servers in each zone, please provide detailed information about potential solutions using containers/micro services?

b) What are the various hosting options available for the proposed solution(s) that allow for data to reside, and remain within Canada (e.g., Software as a Service (SAAS), Infrastructure as a Service (IAAS), Platform as a Service (PAAS), on-premise instances, etc.)?

1. What availability, recovery point objectives, and recovery time objectives can we expect from a SaaS?
2. For a SaaS solution

a) How would you ensure that privacy and confidentiality are protected?

b) How does the potential solution address IT security?

c) What mechanisms/processes are in place

(1) To prevent unauthorized access or data integrity compromise?

(2) For logging and auditing user events, rule / algorithm changes and AI algorithm decisions?

(3) To handle access control and at what level of granularity (e.g., field level, case level, decision level)?

(4) To protect our data?

(5) To package, and transfer data back to the Government of Canada if the solution is discontinued?

(6) For reporting security incidents, and violations?

c) What challenges do you foresee in developing, and implementing this solution, and what solutions exist to overcome those challenges? What are the unique considerations in the government setting? How would you address having separate networks (unclassified, Protected-B, Secret) that cannot communicate with each other.

d) Artificial Intelligence(AI) – Machine Learning (ML)

i) How can AI/ML models be developed to ensure biases or potential biases are not introduced? How are biases detected?

ii) How would industry address the challenge of demands to make AI/ML models transparent to ensure that the predicted outcomes can be reviewed, and the rationale understood (e.g., which factors were the most important in influencing the predicted outcome, and how was the predicted outcome developed)? What would be the consequences in this context of releasing such information?

iii) What solutions do you consider to be mature, developing or in the early stages of implementation that are appropriate for the identified requirements? Are solutions available to meet the identified requirements, or could solutions be customized or configured to meet these requirements? Should solutions not be available to meet identified requirements - could a solution(s) be developed with available AI/ML technology? Please explain.

iv) Can you measure accuracy of predictions of outcomes/trends such as by a margin of error? If yes, what is the margin of error?

v) Explain how efficiency, accuracy, and reliability of such solutions would be ensured and measured? Please explain including in relation to the solutions analytical and predictive capabilities?

vi) Can you correlate across multiple technology domains (compute, network, cloud, storage etc.)?

vii) How does your solution support maintenance windows and change management? Can it pull the information from the ITSM change management tool (e.g. Service Now, Remedy ARS, IBM SmartCloud…)?

viii) Can your solution identify the root cause of an incident based on previous incidents? Does all of the information reside in your solution, or can you pull the data from our ITSM tool?

e) What are the industry's standards, best practices, or measures that can be used to assess the efficiency, accuracy, reliability, and performance of such monitoring solutions?

i) As monitoring is a critical solution, explain how efficiency, accuracy, and reliability of such solutions would be ensured, and measured, especially if a SaaS solution is used.

ii) Please provide a proposed responsibility assignee matrix (RACI) from a provider, and SSC perspective.

RACI is defined as follow:

R = Responsible
A = Accountable
C = Consulted
I = informed

f) Does your solution support integration based on open standards based Representational State Transfer (REST) web services?

g) Are we able to export knowledge data from your solution into our ITSM tool?

h) Is the technology agent based or agentless?

i) What are the advantage and disadvantages?

i) Please provide an overview of the training, and support services available, including considerations for implementing the solution across Canada, potentially across different government departments, and possibly overseas in future iterations.

j) What would be the expected length of time required to provide a solution that meets the aforementioned requirements?

k) Please describe the options for the intellectual property rights, taking into account the viable business models for the solutions, such as vendor-owned, and GC-owned.

l) Please describe the options for the pricing model for a vendor-owned solution (e.g., perpetual license, subscription-based license, user license, device/CPU/server license, entity/enterprise license, other model)?

i) Provide indicative per unit pricing using the sample inventory provided below for event monitoring, runbook automation & AIOPS

ii) How would a cost per unit be done for APM? Please provide indicative pricing for such a solution?

m) Please provide detailed information on APM solutions that can monitor home-grown, as well as COTS applications.

n) Please provide detailed information on how this solution could be integrated into our major tools.

o) Provide examples and details on how this solution can enrich event data from the CMDB as well as leverage a third party ITSM tool as the system of record for incidents.

p) Describe the interface and authentication model that will allow application and/or infrastructure owners to update the monitored parameters, and rules.

q) SSC is currently capturing relationship data from the partner organizations, business application(s), software, DB/web/middleware instances to infrastructure. Redundancy exists within the infrastructure (e.g. dual network interfaces, Redundant Array of Interdependent Disk(s) (RAID) disk, site to site replication, clustered servers/database, and/or load balanced services/appliances). How can your technology allow for SSC to gain insight by leveraging the data in the CMDB and network topology, into what customer/business application is in jeopardy or actual down taking into consideration the redundancy built into the environment?

r) For the dashboard, and portal, please identify, and elaborate if the solution(s) have been assessed against one or more of the following Accessibility Standards: EN 301 549, WCAG 2.0, WCAG 2.1, U.S. Section 508 (Post 2016), Section 508 (Pre 2016), WCAG 1.0.

3. Supplier Responses

3.1 Submitting a Response

a) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should submit it by email to the Contracting Authority at the email address for submitting a response identified on the cover page by the closing date and time identified on the cover page of this document.

b) **Responsibility for Timely Delivery**: Each supplier is solely responsible for ensuring its response is delivered on time to the correct email address.

c) **Identification of Response**: Each supplier should ensure that its name and return address, the solicitation number, and the closing date are included in the response in a prominent location. The supplier should also identify a representative whom Canada may contact about the response, including the person's name, title, address, telephone number and email address.

3.2 Confidentiality

If a supplier considers any portion of its response to be proprietary or confidential, the supplier should clearly mark those portions of the response as proprietary or confidential. Canada will treat the responses in accordance with the *Access to Information Act* and any other laws that apply.

4. Canada's Review of Responses

4.1 Review of Responses

Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify any draft documents provided with this RFI and its procurement strategy. Canada will review all responses received by the RFI closing date and time. Canada may, in its discretion, review responses received after the RFI closing date and time.

4.2 Review Team

A review team composed of representatives of Canada will review and consider the responses. Canada may hire any independent consultant(s), or use any Government resource(s), to review any response. Not all members of the review team will necessarily participate in all aspects of the review process.

4.3 Follow-up Activity

a) Canada may, in its discretion, contact any suppliers to follow up with additional questions or for clarification of any aspect of a response. Canada's follow-up may involve a request for a further written response or for a meeting with representatives of Canada.