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**
**Place du Portage, Phase III**
**Core 0A1/Noyau 0A1**
**11 Laurier St./11, rue, Laurier**
**Gatineau**
**Québec**
**K1A 0S5**
**Bid Fax: (819) 956-3370**

# LETTER OF INTEREST
# LETTRE D'INTÉRÊT

**Title - Sujet**
GC Managed Security Service (GCMSS)

| | |
|---|---|
| **Solicitation No. - N° de l'invitation**<br>2B0KB-123147/A | **Date**<br>2012-07-31 |
| **Client Reference No. - N° de référence du client**<br>20123147 | **GETS Ref. No. - N° de réf. de SEAG**<br>PW-$$XK-100-24691 |
| **File No. - N° de dossier**<br>100xk.2B0KB-123147 | **CCC No./N° CCC - FMS No./N° VME** |

**Solicitation Closes - L'invitation prend fin**
**at - à 02:00 PM**
**on - le 2012-08-30**

**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:**<br>Menechian, Noubar | **Buyer Id - Id de l'acheteur**<br>100xk |
| **Telephone No. - N° de téléphone**<br>(819) 956-4485 ( ) | **FAX No. - N° de FAX**<br>(819) 956-8303 |

**Destination - of Goods, Services, and Construction:**
**Destination - des biens, services et construction:**
See herein

**Comments - Commentaires**

**Instructions: See Herein**

**Instructions: Voir aux présentes**

**Vendor/Firm Name and Address**
**Raison sociale et adresse du fournisseur/de l'entrepreneur**

| | |
|---|---|
| **Delivery Required - Livraison exigée**<br>See Herein | **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**

**Issuing Office - Bureau de distribution**
Secure Channel Division (XK)/Division de la voie de communication protégée (XK)
12C1, Place du Portage Phase III
11 Laurier St./11, rue Laurier
Gatineau
Québec
K1A 0S5

Canada

# REQUEST FOR INFORMATION

# GOVERNMENT OF CANADA MANAGED SECURITY SERVICE (GCMSS)

# FOR CANADA

## TABLE OF CONTENTS



**Attachment:**
Draft Request for Proposal (RFP)

## A. 1 Background and Purpose

Shared Services Canada (SSC) currently delivers a suite of fully managed perimeter defence services including the existing Managed Security Services (MSS) portfolio to partner departments and Other Government Departments (OGDs). This portfolio of services provides a comprehensive set of solutions covering perimeter security, intrusion detection and content filtering for web and email. These services can be combined with existing GC-owned solutions for holistic protection of departmental public access zones.

MSS is presently procured under the Secure Channel contract that will end in December 2013. Consequently, this Government of Canada Managed Security Servcice (GCMSS) procurement initiative has been initiated to competitively tender these services and transition existing MSS clients to GCMSS by December 2013.

The existing MSS deployment architecture is comprised of centralized and distributed solutions as shown in Figure 1. The centralized solution is located into the Contractor's data center and delivers the Antivirus and the Antispam services to the subscribing client departments using department's specific policies. The centralized solution is based on Cisco IronPort Email Security Appliances. The distributed solution is located into individual departments Public Access Zone (PAZ) within their data center. The distributed solution is based on Fortinet Fortigate and Cisco ASA UTM appliances to deliver Firewall and Intrusion Detection services and WebSense Web Filter to deliver content filtering.

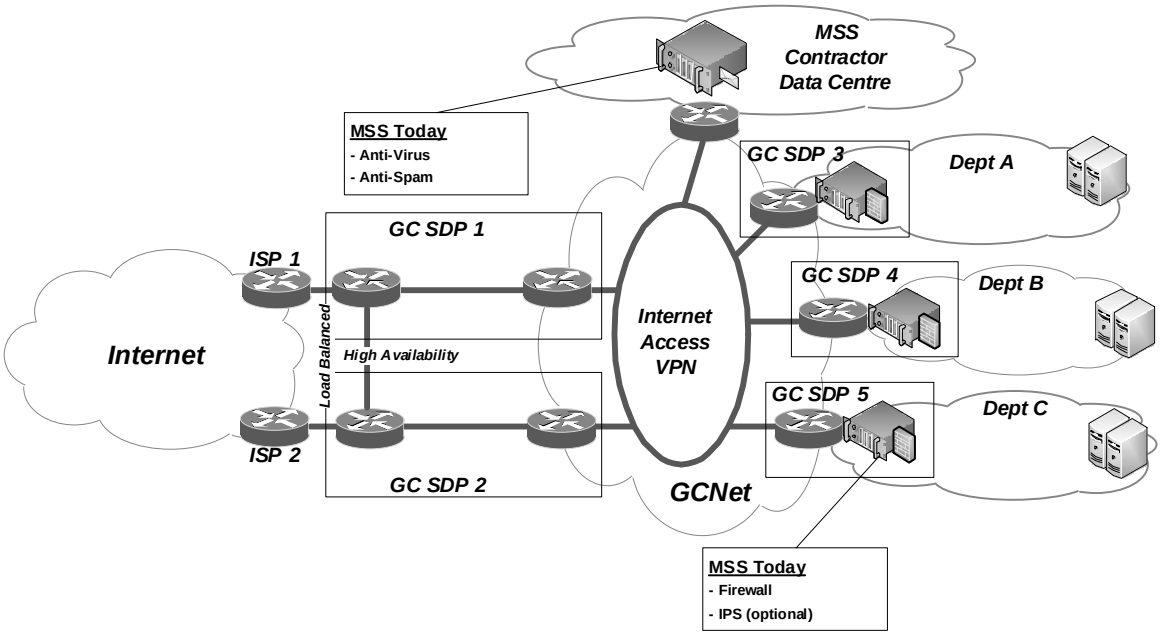


**Figure 1 - MSS Deployment Architecture**

## A. 2 Service Objectives

The objectives for the Government of Canada Managed Security Service (GCMSS) are:

(a) reduce operational and management costs;

(b) offer a scalable service to meet the demand;

(c) offer a secure and private service compliant to security and privacy policies;

(d) provide a flexible and agile solution that can:

(i) adapt to the constantly changing threat landscape; and

(ii) support multiple deployment scenarios;

(e) decrease power and space requirements in the data center; and

(f) complement technical security with end-user security-minded behaviours.

**A. 3 Business Assumptions**

The business assumptions for the GCMSS service are:

(a) implemented at Canada's locations as specified by Canada;

(b) allow smooth transition of existing MSS users;

(c) accredited for Protected "B"; and

(d) no need for instructor led training.

**A. 4 Business Requirements**

(a) Shared Services Canada (SSC) has a business requirement to replace the existing MSS portfolio with a Government of Canada Managed Security Service (GCMSS) that is flexible and agile while taking into account SSC business and technical requirements as well as evolution of the industry. The GCMSS will provide departments with IT infrastructure and services that mitigate security risks associated with connecting to unprotected or untrusted networks, such as the Internet, while enforcing security and usage policies compliance as indicated by the Treasury Board Secretariat (TBS).

The resulting contract will be for fully managed services that may include centralized as well as distributed implementations of the following security services:

- Firewall
- Intrusion Detection and Prevention
- Content Filtering
- Antivirus
- Antispam
- Data Loss Prevention
- Security Information and Event Management

The contract will also offer provisions for the following on-demand services, in direct support of the aforementioned security services:

- Security Awareness Training
- Integration Support

The following Table provides a brief description of each of the services for MSS.

| Security Service | Description |
|---|---|
| Firewall | Acts as a safeguard for Canada's information assets from electronic threats originating from within the government of Canada as well as threats posed by connection to a non-trusted network, such as the Internet. |
| Intrusion Detection/Prevention | Monitors Canada's network traffic in real-time for hostile activity and alerts Canada to organized attacks or security breaches at the earliest stage and takes appropriate action. |
| Content Filtering | Scans Internet traffic and requests and may obstruct access to undesirable Internet sites and content through standardized policies thereby supporting Canada's acceptable use policy. |
| Antivirus | Protects against malicious code by filtering inbound and outbound traffic to block infected files. |
| Antispam | Provides inbound and outbound Spam email capture for filtering and blocking of phishing attempts. |
| Data Loss Prevention | Identifies, monitors, and protects data in endpoint actions and network actions, thereby detecting and preventing unauthorized use and transmission of confidential information while enforcing related internal policies. |
| Security Information and Event Management | Collects, analyzes and correlates log information from numerous sources across the enterprise, including strategically placed sensors, so as to advise the client on critical security incidents and events while providing forensic reporting and documentation capabilities. |

**Table 1 - Managed Security Services**

It should be noted that there is no intended service overlap between the Email Transformation Initiative (ETI) project and the Government of Canada Managed Security Service (GCMSS) RFP. GCMSS is intended to extend the lifetime of existing fully-managed perimeter defence services as provided under the Secure Channel contract, which will end on December 31, 2013.

In contrast, SSC has launched the Email Transformation Initiative (ETI) with the primary strategic objective to replace existing email systems distributed across all SSC Partner departments with a consolidated email solution. Given the anticipated lifetime of the GCMSS contract and differing scope, SCC does not intend to leverage GCMSS as part of the ETI project.

## A. 5 Conceptual Model for GCMSS

The conceptual model of the GCMSS shown in Figure 2 proposes, for information purposes only, a distribution of the Threat Management Services that is somewhat similar to the existing MSS. The Threat Management Services are represented into two categories:

(a) Centrally hosted services - on shared or common high-availability appliances at Canada-owned Internet control point; and

(b) Distributed services - on dedicated standard or high-availability appliances located on Client Organization premises.

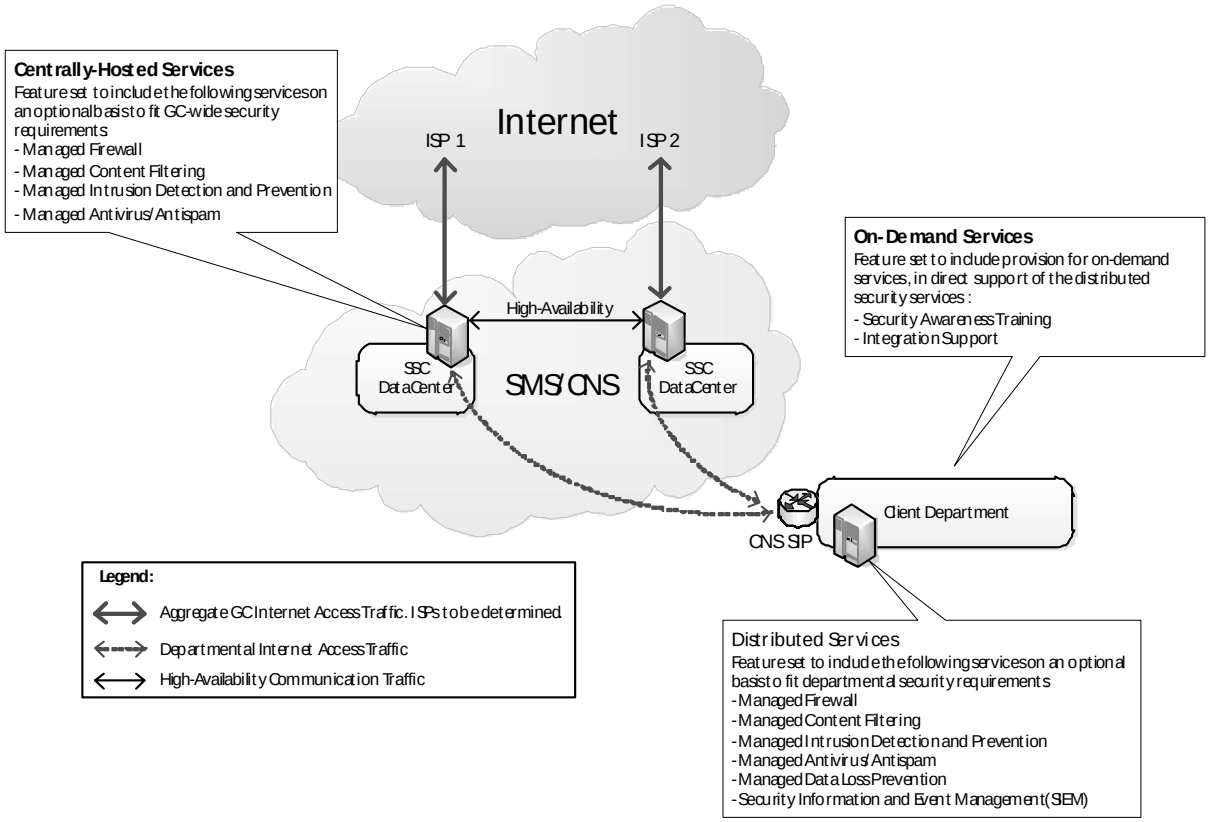


**Figure 2 - GCMSS Conceptual Model**

All Threat Management Services must be able to work in conjunction with each other, as well as, pre-existing Client Organization-owned and/or Shared Services Canada-owned security services to facilitate transition.

Capacity at each centralized Service Delivery Point (SDP) must be sufficient to handle all Internet traffic in the event of the loss of an ISP (i.e., must support the Internet access high availability architecture).

## A. 6 Potential Deployment Scenarios

The actual deployment of GCMSS could be accomplished using multiple deployment scenarios. Canada identified 3 potential deployment scenarios that could be viable for the implementation of GCMSS recognizing that some Client Organizations will be more suited to a distributed approach, while others will be better suited to a centralized approach.

For more details, please see Attachment 2.2 Service Model of the RFP.

## A. 7 Purpose of this Request for Information (RFI)

The purpose of this Request for Information (RFI) is to consult with Industry on specific areas of interest related to the implementation of this new GCMSS. It is expected that Industry will review it and provide further guidance and feedback to ensure a subsequent fair and equitable RFP solicitation.

## A. 8 Nature of Request for Information

This is not a bid solicitation. This RFI will not result in the award of any contract. As a result, potential suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Nor will this RFI result in the creation of any source list. Therefore, whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to the matters described in this RFI.

## A. 9 Nature of Responses Requested

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

## A. 10 Response Costs

Canada will not reimburse any respondent for expenses incurred in responding to this RFI.

## A. 11 Treatment of Responses

(a) **Use of Responses**: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify procurement strategies or any draft documents contained in this RFI. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.

(b) **Review Team**: A review team composed of representatives of the client (where applicable) will review the responses. Canada reserves the right to hire any independent consultant, or use any Government resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

(c) **Confidentiality**: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the *Access to Information Act*.

(d) **One-on-One Follow-up Activity**: Canada will meet with any respondent upon request. Following the closing date, the Contracting Authority will follow up individually with all respondents who indicate in their responses that they wish to meet with Canada.

## A. 12 Contents of this RFI

(a) This RFI contains the draft Request For Proposal, its attachments, Statement of Work (SOW) and its appendices. This document remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the draft document are welcome.

(b) This RFI also contains specific questions addressed to Industry.

## A. 13 Questions to Industry

Respondents to the RFI are asked to respond to the questions in this section in the context of the material presented in sections A.1 to A.6.

(a) **Question 1**

Please comment on any obstacles, impediments and/or delivery risks for the GCMSS objectives, business requirements, assumptions and the conceptual model.

(b) **Question 2**

Please comment on the similarities with respect to the business objectives and requirements that your proposed solution has in comparison with your existing commercial offerings.

(c) **Question 3**

To effectively achieve ease of business management with minimal administrative overhead, Canada requires a pricing model based on a one-time price to install at a site, a one-time price per feature and low recurring payments. Please comment on the viability of this approach, as well as any alternate commercial and/or cost-effective solutions that may apply.

(d) **Question 4**

To facilitate ease of deploying new sites, as well, as upgrading existing sites with new features, Canada requires the service to have the capacity to operate at wire speed with all potential features turned on. Please comment on the viability of this approach, as well as any alternate commercial and/or cost-effective solutions that may apply.

(e) **Question 5**

Please comment as to how your proposed reporting portal aligns with commercially available solutions and provides support for related reporting features such as support for departmental Syslog servers and integration with Information Protection Center (IPC) communication processes.

How much customization is required to bring your proposed solution to commercial readiness?

(f) **Question 6**

Please comment as to how your proposed managed service maintains in-band and out-of-band secure remote management of solutions that might be logically located in departmental public access and/or operational zones.

(g) **Question 7**

Please comment on the similarities that your proposed managed Security Information and Event Management (SIEM) service has in comparison with your existing commercial offerings.

How much customization is required to bring your proposed solution to commercial readiness?

(h) **Question 8**

Please comment on the similarities that your proposed managed Data Loss Prevention (DLP) service has in comparison to existing commercial offerings.

How much customization is required to bring your proposed solution to commercial readiness?

(i) **Question 9**

Please comment on the similarities that your proposed managed security awareness training service has in comparison to existing commercial offerings.

How much customization is required to bring your proposed solution to commercial readiness?

(j) **Question 10**

Based on a scenario where Canada runs both IPv4 and IPv6 services, please comment on the following aspects of your solution:

(i) IPv6 capability (e.g. BCP 38, RFC 3704);

(ii) service gaps between IPv4 and IPv6;

(iii) IPv6 interoperability challenges amongst a multi-vendor solution (components/parts/boxes) and Canada's network;

(iv) performance differential between IPv6 and IPv4 services; and

(v) IPv4 to IPv6 transition mechanisms: translation and tunneling.

(k) **Question 11**

The US National Information Assurance Partnership (NIAP) has a program, the Common Criteria Evaluation and Validation Scheme (CCEVS), to evaluate IT product conformance to international standards. NIAP is in the process of replacing the existing Evaluation Assurance Levels (EALs) with new technology specific Protection Profiles (PP). New PP are under development and will not be available before the end of 2012.

In that context, please comment on how you would ensure commitment from your original equipment manufacturer (OEM) to certify their products against the new NIAP approved PP, as they become available, so their products will be on the Product Compliant List.

Please comment as to how Canada could address that product certification timing issue against upcoming PP in the GCMSS SOW.

(l) **Question 12**

As per the Merx posting (2B0KB-12NNSE/A) on May 28, 2012, Shared Services Canada plans to apply the National Security Exemption (NSE) to procurements related to network/telecommunications. Given the criticality of the service to Canada's National Security, this will include GCMSS. Please comment on the following GCMSS NSE requirements:

(i) Bidder's ownership and control must be 100% Canadian as well as any subcontractors;

(ii) Data must reside and be routed within Canada at all times; and

(iii) Proposed equipment must be approved by the Communications Security Establishment of Canada (CSEC).

(m) **Question 13**

Please comment on how your proposed managed security services could be extended to include mobile devices?

How much customization is required to bring your proposed solution to commercial readiness?

**A. 14 Format of Responses**

(a) **Cover Page**: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

(b) **Title Page**: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

(i) the title of the respondent’s response and the volume number;

(ii) the name and address of the respondent;

(iii) the name, address and telephone number of the respondent’s contact;

(iv) the date; and

(v) the RFI number.

(c) **Numbering System**: Respondents are requested to prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

(d) **Number of Copies**: Canada requests that respondents submit 2 hard copies and 1 soft copy of their responses.

**A. 15 Enquiries**

Because this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all potential suppliers. However, respondents with questions regarding this RFI may direct their enquiries to:

| | |
|---|---|
| Contracting Authority: | Noubar Menechian |
| E-mail Address: | noubar.menechian@ssc-spc.gc.ca |
| Telephone: | (819) 956-4485 |
| Facsimile: | (819) 956-5165 |

## A. 16 Submission of Responses

(a) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should deliver it to the following location by the time and date indicated on page 1 of this document:

Bid Receiving Unit
Portage III, 0A1
11 Laurier Street
Gatineau, Quebec K1A 0S5

Fascimile: (819) 997-9776

**Responses should not be sent directly to the Contracting Authority.**

(b) **Responsibility for Timely Delivery**: Each respondent is solely responsible for ensuring its response is delivered on time to the correct location.

(c) **Bid Receiving Unit Address Solely for Delivery of Responses**: The above address is only for bid submission. No other communications are to be forwarded to this address.

(d) **Identification of Response**: Each respondent should ensure that its name and return address, the solicitation number and the closing date appear legibly on the outside of the response.