REQUEST FOR INFORMATION (RFI) FOR DATABASE SECURITY SOLUTIONS

TABLE OF CONTENTS

SECTION A - Overall Objectives 3
A1.0 RFI Objective 3
SECTION B - Submission of Responses 3
B1.0 Response Preparation Instructions 3
B2.0 Authorities 4
B2.1 Contracting Authority 4
B3.0 Industry Information Session 4
B3.1 Interactive Vendor Demonstration Sessions 4
B4.0. Industry Responses 5
B4.1 Response Format 5
B4.2 Language of Response 5
B4.3 Response Parameters 5
B4.4 Response Confidentiality 5
SECTION C – Procurement Strategy 5
ANNEX A – Response Requirements 6
1. Corporate Profile 6
2. Solution Description 6
3. Questions 7
Table 1 - Architectural Questions 7
Table 2 - Functionality Questions 7
Table 3 - Integration Questions 9
Table 4 - Support Questions 10
Table 5 - Standards Questions 11
Table 6 – Licensing Questions 11
4. Alternative Suggestions 11
5. Demonstrations 11
Appendices 12
Appendix A – CBSA Technical Environment Information 12

SECTION A - OVERALL OBJECTIVES

A1.0 RFI OBJECTIVE

The Canada Border Service Agency (CBSA) is investigating options that will provide security and auditing functionality to its data holdings. The key objective of this RFI is to obtain Vendor feedback on an available "off the shelf" Solution that enables enterprise-scale data security policy management specific to the needs of the CBSA. This will allow the CBSA to get an idea of the type of commercially available solutions on the market and their capabilities.

Note: The Solution proposed and referenced in responses to the provide questions must be currently commercially available.

SECTION B - SUBMISSION OF RESPONSES

B1.0 RESPONSE PREPARATION INSTRUCTIONS

B1.1 The CBSA requests that Vendors provide their responses in separately bound sections as follows:

a. Provide one hard copy and one soft copy on CD in a Microsoft Word Format. The CBSA requests that Vendors follow the instructions described below in the preparation of their response:
   i. use 8.5 x 11 inch (216 mm x 279 mm) paper; and
   ii. use a numbering system that corresponds to the RFI.

b. In accordance with the Policy on Green Procurement. In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Vendors should:

   i. use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and

   ii. use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

B1.2 Vendors are requested to submit responses by: October 16, 2014

B1.3 Vendors **must** submit enquiries and responses to this RFI using the following delivery address:

Delivery Address: Canada Border Service Agency
Cheque Distribution and Bids Receiving Area
473 Albert Street, 6th Floor
Ottawa, ON K1A 0L8
Bid Receiving Unit is open from Monday to Friday inclusively, between the hours of 08:30 AM to 11:30 AM, excluding Statutory Holidays.

B1.4 The review of responses will begin after the date and time mentioned above. Responses received after that date may not be reviewed.

B1.5 In the event that a response is not sufficiently clear, the CBSA reserves the right to seek additional information at their sole discretion.

B2.0 AUTHORITIES

B2.1 CONTRACTING AUTHORITY

The Contracting Authority is responsible for the management of the procurement and RFI process.

Aleksandra Green
Contracting Officer
Comptrollership Branch
Canada Border Services Agency
473 Albert Street
Ottawa, ON K1A 0L8
Telephone: 613-960-3350
E-mail address: aleksandra.green@cbsa.gc.ca

B3.0 INDUSTRY INFORMATION SESSION

B3.1 INTERACTIVE VENDOR DEMONSTRATION SESSIONS

The CBSA may at its sole discretion entertain meetings with interested respondents to provide them with the opportunity to present/demonstrate/discuss their capabilities in relation to this RFI.

Respondents that have expressed such interest can expect to be contacted within approximately 2 weeks of the RFI closing date to schedule the vendor session. An Invite Agenda along with specific questions or areas of interest to be covered during the session will be provided to the invited respondents.

The vendor session will be located in the National Capital Region. The exact location and timeframe will be detailed in the Invite Agenda. Vendors will also be asked to provide an electronic version of their presentation.

The vendor session will cover specific functional and technical aspects of Database Security COTS Software. As such, vendor representatives attending the session must include Subject Matter Expert(s) in these areas in order to meaningfully respond to questions at the session. The CBSA personnel with extensive experience in IT technology will attend the presentation.

B4.0. Industry Responses

B4.1 Response Format

For ease of use and in order that the greatest value be gained from responses, Canada requests Vendors to follow the structure outlined in ANNEX A – Response Requirements.
There is no page limit on the information to be provided.

B4.2 Language of Response

Responses may be in English or French, at the preference of the Vendor.

B4.3 Response Parameters

Vendors are reminded that this is an RFI and not a Request For Proposal (RFP) and in that regard, Vendors should feel free to provide their comments, concerns, and, where applicable, alternative recommendations on how the requirement may be satisfied.

B4.4 Response Confidentiality

Vendors are requested to clearly identify those portions of their response that are proprietary to the Vendor. The confidentiality of each Vendor's response will be maintained.

SECTION C – Procurement Strategy

At present, the CBSA does not have any plans to solicit a RFP. This RFI is for the sole purpose of gathering information as described in Section A.

ANNEX A – RESPONSE REQUIREMENTS

The purpose of this RFI is to obtain detailed information from the Vendor community. The CBSA has outlined below a list of questions and are requesting Vendors to respond in detail, so that the CBSA can compile information about the Data Security products available in the current market place.

This RFI is not a commitment with respect to future purchases or contracts. Note: The Solution proposed and referenced in responses to the provide questions must be currently commercially available. In preparing their responses the Vendor community should refer to Appendix A – CBSA Technical Environment Information.

The CBSA is asking the Vendor community to provide the following:

1. CORPORATE PROFILE

Each Vendor should provide the following information:

a. Company name, address, telephone & fax numbers and e-mail address.
b. Company contact name and telephone number.
c. Company background information (location of parent company, contact information for company representative and or distributor in Canada if any, type of product sold and web site address. The CBSA may ask for additional contact information at any point in time.

2. SOLUTION DESCRIPTION

Each Vendor should provide the following information:

a. A Solution identifier such as a model number, version number and a description of all components required for the Solution;
b. Brochures outlining the specifications and details of the equipment should be included in the response to this letter of interest;
c. Costing model;
d. Licensing model; and
e. Support and Maintenance Service Levels.

3. QUESTIONS

The CBSA is asking the Vendor community to respond to the questions below.

TABLE 1 - ARCHITECTURAL QUESTIONS

CBSA Question	Vendor Response
1. How will your Solution integrate into and provide its complete functionality set, inclusive of the ability to enable the CBSA to monitor, control, and audit access to its data, across its complete environment? (Refer to "Appendix A- CBSA Technical Environment Information" for "complete environment" information)	
2. How does your Solution provide the CBSA with the ability to protect its data from internal and external web based applications and any special integration needs required, to obtain full functionality of your Solution? (Refer to "Appendix A- CBSA Technical Environment Information" for "special integration needs required" information)	
3. How will your Solution provide its full functionality without causing any additional load in terms of CPU or Memory consumption on existing databases, new database, and application servers?	

TABLE 2 - FUNCTIONALITY QUESTIONS

CBSA Question	Vendor Response
4. How does your Solution deal with the following challenges associated with data and database security? a. User access and access control. How does your Solution segregate or control user access to data? b. Audit logs. Does your Solution produce audit records that capture at a minimum the following events performed by user, service, and system accounts? i. Type (e.g. login, logoff,	

CBSA Question	Vendor Response
configuration changed); ii. When (e.g. 2013-01-01 5:00am EST); iii. Where (e.g. system ID); iv. Source (e.g. workstation ID); v. Outcome (e.g. success, fail); and vi. Identity (e.g. user account ID, service account ID, system account ID). c. Does your Solution audit accesses with elevated privileges, such as an administrator or system administrator account? d. Does your Solution notify administrators and perform configured recovery actions if your Solutions audit service fails or is inadvertently turned off? If so, please describe how. e. Does your Solutions exception handling service log all exceptions and failure events to an exception log? f. How are audit logs accessed by authorized users and how they are secured against unauthorized access, modification and deletion? g. Does your Solution generate reports for audit records in a readable format? h. Is your Solution able to send audit records to a central repository? i. Does your Solution support encryption of user IDs and passwords between a client device and servers? j. Does your Solution generate time stamps for audit records? If so, do they use internal system clocks and do they contain both date and time including seconds? If so, is the time expressed in Coordinated Universal Time (UTC) or local time with an offset from UTC? If	

CBSA Question	Vendor Response
so, is your Solution able to synchronize its time with a client defined authoritative time source? k. Where are the audit logs stored within your Solution, or can this be customized? l. Does your Solution permit the configuration of an audit log retention period? m. Does your Solution audit read access of data by users and administrators within your Solution?	
5. How does your Solution allow for administration of all default passwords and privileges of user, service, and system accounts?	
6. Can your Solution be hardened, which includes the ability to disable or remove unnecessary components, services, and user IDs and passwords? If so, please describe how this would be achieved.	
7. How does your Solution provide continuous monitoring access to all sensitive data and raise real time alerts from critical violations? How does it define and identify them?	
8. Does your organization have in place a process that identifies security patches and fixes for your Solution? If so, how are these security patches fixes made available?	
9. Does your organization have in place a process that identifies vulnerabilities in your Solution? If so, how are required remediation actions to address these vulnerabilities made available?	
10. Do you provide administrator and user documentation for your Solution, including applicable hardening guides? If so, please describe what they address.	

TABLE 3 - INTEGRATION QUESTIONS

CBSA Question	Vendor Response

CBSA Question	Vendor Response
11. Does your Solution integrate with IBM z/OS identification, authentication, and authorization services and protocols (e.g. Access Control Facility; Resource Access Control Facility)? If so, please describe how.	
12. Does your Solution integrate with Microsoft Windows Active Directory identification, authentication, and authorization services or protocols (e.g. Lightweight Directory Access Protocol; Kerberos)? If so, please describe how.	
13. Does your Solution integrate with Microsoft Windows Group Policy Objects? If so, please describe how.	
14. Does your Solution integrate with Tivoli Endpoint Manager and Microsoft Windows Software Update Service)? If so, please describe how.	
15. Does your Solution integrate with McAfee Host Intrusion Prevention, McAfee Policy Auditor, and McAfee VirusScan Enterprise with Anti-Spyware managed through McAfee ePolicy Orchestrator? If so, please describe how.	
16. Does your Solution provide for secure communications of critical event notifications, or can they be customized? If so, please describe how.	
17. Does your Solution provide for management through secure connections that utilize an IPSec AES-256 connection, TLS v1.1 or higher with SSL v3.0 or higher protocols, or SSH v2.0 or higher? If so, please describe how.	
18. Does your Solution require connectivity to or a link from your network infrastructure?	

TABLE 4 - SUPPORT QUESTIONS

CBSA Question	Vendor Response
19. How do you provide support for your Solution, including the application of security patches and fixes, the implementation of	

CBSA Question	Vendor Response
known vulnerability remediation actions, and the troubleshooting and resolution of incidents or problems with cryptographic modules (if applicable)?	

TABLE 5 - STANDARDS QUESTIONS

CBSA Question	Vendor Response
20. Have the cryptographic modules (if applicable) provided by your Solution been validated and certified by the Cryptographic Module Validation Program (CMVP) to at least Federal Information Processing Standards (FIPS) FIPS 140-2?	
21. Is your Solution able to support Government of Canada (GoC) public key infrastructure standards, such as Entrust Digital ID and Microsoft?	

TABLE 6 – LICENSING QUESTIONS

CBSA Question	Vendor Response
22. How do you typically license your COTS Software? (i.e. types of users, by servers, by CPU, concurrent users, enterprise-wide)?	
23. How many individual licenses would need to be purchased in order to trigger the licenses to become an enterprise-wide licence?	

4. ALTERNATIVE SUGGESTIONS

Do you (the Responder) have any suggestions and or concerns with respect to the tasks and questions listed in Annex A? If so, please outline your suggestion(s), concern(s) and any recommendations to resolve them.

5. DEMONSTRATIONS

Would your company be interested in attending a RFI follow-up session with the opportunity to demonstrate your COTS Software? The session can be held on-site at the CBSA or remotely utilizing web/video conferencing. See "Interactive Vendor Demonstration Sessions" for more details.

APPENDICES

APPENDIX A – CBSA TECHNICAL ENVIRONMENT INFORMATION

Background

The Canada Revenue Agency (CRA) and Shared Services Canada (SSC) currently provide infrastructure services to the CBSA.

Windows "Managed" Environment

The Distributed Computing Environment (DCE) is a Client and Server based Infrastructure that consists of Windows based servers, desktops and laptops with Windows Active Directory (AD) providing the backend directory services. There are approximately hundreds sites across Canada supported by the DCE. These sites will vary in size from as little as two Users upwards of hundreds in a single building. Bandwidth at these sites also varies. A typical distributed site is comprised of a File and Print server and possibly an Exchange server. Exchange services will be completely centralized by 2015. Local File and Print services are also under review to port to centralized services. Local or centralized AD domain controllers facilitate the directory services for the managed environment.

The CBSA also leverages the Terminal Services Platform (TSP) using Citrix, which consists of central servers located in the National Capital Region hosting a variety of applications and services for a select group of Users. These applications and services include specific line-of-business applications along with base productivity applications such as MS Office, Outlook and Exchange, host emulator SW (Attachmate) and basic File and Print Services to name a few. In addition the CRA utilizes Softgrid application virtualization SW to enhance application access and management within the TSP farm.

The following bullets will highlight the key Windows based software installed within the CBSA DCE.

- MS Windows 2008 Server
- Citrix XenApp
- Windows 7 Enterprise SP1 32bit (includes BitLocker)MS Office 2010
- MS Exchange 2010
- Entrust Security Provider 9.2 and Entrust Security Provider for Outlook 9.1
- Current McAfee Anti Virus v8.8 /w Anti-Spyware, Intrusion Prevention v8.0, Policy Auditor 6.0 managed through McAfee ePO services.
- Tivoli Endpoint Manager for software deployment, Inventory, and Remote Control.
- Microsoft WSUS for platform patch currency

The current version of the Java Runtime Environment (JRE) installed on each desktop is version 1.6.0_18, upgrading to version 1.7.

The underlying hardware for the Windows environment consists of servers based on AMD and Intel architectures using multi core and multi-processor technology. Desktops and Laptops are also based on AMD and Intel architectures using multi core processors and dual channel memory.

The platform is considered "managed" since all workstations comply with the standard suite of security tools and monthly OS patch cycles. Additionally, every device is created as an object within the AD directory. Devices are there subjected to the mandatory policies associated to securing the device. Policies such as login script execution, local administration, and role based access are assigned to each device registered within the domain. Customization of policies can be accommodated and is for many of the CBSA's "niche" device requirements. Additionally, critical and mandatory software deployments can be accommodated in an automated fashion via the Tivoli suite.

Database Environment

The CBSA's data holdings are based on both Mainframe Z/OS in a SYSPLEX configuration and Linux/Unix/Windows (LUW) environment based across dual datacenters for failover reasons;

Data is stored in:

- DB2-Z/OS;
- DB2-LUW;
- DB2(MPP) –LUW;
- Sql-Server;
- Sybase;
- Postgres; and
- Puredata DB Appliance
- As well as non-DB based data (VSAM, PDF, Flat file, etc...).

Applications are based on 2 and 3 tier Client Server architecture.