RETURN INFORMATION TO:

By Email:

nc-solicitations-gd@hrsdc-rhdcc.gc.ca

(Size limit – 13MB)

REQUEST FOR INFORMATION

Comments:

This is not a bid solicitation but an inquiry for the purpose of obtaining information for the goods, services, and construction specified herein. The information requested herein is for budgeting and planning purposes only.

Contracts will not be entered into on the basis of suppliers' responses.

Instructions : See Herein

Issuing Office:

ESDC
Employment and Social Development Canada
140 Promenade du Portage,
Gatineau, QC, K1A 0J9

Title: RFI – CYBER THREAT PREVENTION	
Solicitation No.: 100021580	**Date:** September 23, 2022
File No. – N° de dossier:	
Solicitation Closes **At 02 :00 PM / 14 h** ***Friday, October 7, 2022***	**Time Zone** Eastern Daylight Savings Time(EDT)
Address Inquiries to : Marco Quiroga nc-solicitations-gd@hrsdc-rhdcc.gc.ca	
Destination: See Herein	

Vendor/firm Name and address :   **Facsimile No. :**   **Telephone No. :**   **E-mail :**   **Procurement Business Number (PBN) :**
Name and title of person authorized to sign on behalf of Vendor/firm (type or print):   **Name:**   **Title:**   **Signature:**   **Date:**

REQUEST FOR INFORMATION

1.0 BACKGROUND AND PURPOSE OF THIS REQUEST FOR INFORMATION

A) OBJECTIVE

The purpose of the Request for Information (RFI) is to collect information on suppliers who provide subscription type of information on cyber threat prevention, protection, response, and recovery and provide all of the services listed in the Annex A – Requirements, including benchmarks, scanning tools, guidelines and other related information on secure configurations related to secure cloud initiatives.

B) BACKGROUND

The Cyber and IT Security part of the Innovation, Information and Technology Branch of Employment and Social Development Canada (ESDC) is responsible for supporting secure cloud initiatives for the department. As part of this work, they have for many years had a subscription through Shared Services Canada to a service provided by the Center for Internet Security (CIS), an independent, nonprofit organization that provides access to information on cyber threat prevention, protection, response, and recovery. In the last year, ESDC has obtained a membership on its own which has provided it with up-to-date information drawn from world-wide experts on benchmarks, scanning tools, guidelines and other related information on secure configurations related to secure cloud initiatives. ESDC has used this information to accelerate IT Security service delivery and to improve the overall quality and completeness of its deliverables in terms of secure cloud initiatives.

The Cyber and IT Security organization has a continuous need for assistance in installing and using security scanning tools to secure the organization and to secure specific platforms. These tools allow administrators to ensure that the computers in the network have their security configuration set to an accepted industry standard. In addition, there is an ongoing requirement for vendor-neutral configuration guides; updates related to data protection, account management, access control management, audit log management, email and web browser protections and others.

C) PURPOSE

This RFI seeks industry feedback to:

1. Collect information on availability for similar services as those described in the Annex A, Requirements;
2. Receive responses from the vendor community about their services;
3. Solicit vendors to provide an interactive demonstration of how their services address the listed questions, and to discuss their services in detail; and
4. Obtain access for a 2-month period for ESDC to further examine the services and how they meet the needs of Cyber and IT Security in their work.

Additionally,

This RFI is neither a call for tender nor a Bid Solicitation. No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way a commitment by the Government of Canada, nor as authority to potential respondents to undertake any work

that could be charged to Canada. This RFI is not to be considered as a commitment to issue a subsequent solicitation or award contract(s) for the work described herein. Although the information collected may be provided as commercial-in-confidence (and, if identified as such, will be treated accordingly by Canada), Canada may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third party or personal information. Please note that Canada may be obligated by law (e.g., in response to a request under the Access of Information and Privacy Act) to disclose proprietary or commercially-sensitive information concerning a respondent (for more information: http://laws-lois.justice.gc.ca/eng/acts/a-1/).

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

2.0 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.

3.0 SCHEDULE

In providing responses the following schedule should be utilized as a baseline:

Task	Completion
RFI Submissions Due	October 7, 2022.
Vendor Responses Reviewed	October 12, 2022
Presentations by the Vendors	October 19, 2022
Access to sample products	As outlined in the RFI
Return/ Termination of access to sample products	December 7, 2022

4.0 NATURE AND FORMAT 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.

5.0 RESPONSE COSTS

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

6.0 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 the requirements 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 Canada 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;

(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. https://laws-lois.justice.gc.ca/eng/acts/a-1/

(d)   **Follow-up Activity:** This RFI is for the sole purpose of gathering information as described in Section A. It is expected that ESDC will contact the vendor to request a demonstration of the vendor's service. In such cases the vendor will be provided advance notification of the time and date of the meeting. The demonstration will be completed virtually. The exact timeframe will be detailed in the invite agenda. However, at no time will the session exceed 3 hours in length. The vendor must provide a contact name, email address and telephone number when submitting their response.

The Vendor session will cover specific technical and general details based on the questions identified in this document. As such, representatives attending the session should include business and technical Subject Matter Experts (SMEs) in these areas. ESDC personnel with extensive experience in Information Technology (IT) Security will also attend the presentation.

Vendors are advised to clearly identify which portions of their responses are proprietary. The confidentiality of each vendor's response will be maintained. Due to the nature of RFI activity, respondents must be aware that aspects (that have not been labelled confidential) of their responses may be used as ESDC prepares for any future procurement.

ESDC would also like permission for all vendors participating in the demonstration to provide, for a period of up to two (2) months, access to their subscription service for further examination by ESDC personnel in addition to access to a technical expert.

 Information provided in response to this RFI will be divulged only to individuals authorized to participate in this pre-procurement activity.

Responses to this RFI will not be used to pre-qualify or otherwise restrict participation in any future RFP. Responses will not be formally evaluated.

ESDC will not reimburse any expenditure incurred in preparing responses, providing systems and participating in the demonstration sessions related to this RFI.

7.0 CONTENTS OF THIS RFI

The documentation contained in this RFI remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that may ultimately be 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 documents are welcome.

8.0 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 one (1) copy of their responses.

9.0 ENQUIRIES

All enquiries and other communications related to this RFI must be directed exclusively to the ESDC Contracting Authority This is not a bid solicitation, therefore Canada will not necessarily respond directly to enquiries in writing or by circulating answers to all potential suppliers. However any questions from respondents concerning this RFI must be made in writing to the Contracting Authority stated below, **via e-mail** on or before the closing date.

Name: Marco Quiroga
Title: Procurement Specialist
          Chief Financial Officer Branch, Employment and Social Development Canada
          140 Promenade du Portage, Gatineau, QC K1A 0J9
E-mail Address: NC-SOLICITATIONS-GD@hrsdc-rhdcc.gc.ca

Canada reserves the right to not respond to questions received after the closing date or to any question not related to this RFI. Enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the

questions or may request that the respondent do so, so that the proprietary nature of the question is eliminated, and the responses will be made publicly available through the Government Electronic Tendering Service (https://buyandsell.gc.ca/).

Changes to this RFI may occur and will be advertised through an amendment on the Government Electronic Tendering System. Canada asks Respondents to visit Buyandsell.gc.ca regularly to check for changes, if any.

10.0 SUBMISSION OF RESPONSES

a) Changes to this RFI may occur and will be advertised on the Government Electronic Tending System. Canada asks Respondents to visit Buyandsell.gc.ca regularly to check for changes, if any.

b) **Time and Place for Submission of Responses**: Interested suppliers must send their responses by email to NC-SOLICITATIONS-GD@hrsdc-rhdcc.gc.ca to the Contracting Authority identified above by the time and date indicated on the first page of this RFI.

c) **Responsibility for Timely Delivery**: Each respondent is solely responsible for ensuring its responses are emailed on time.

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

ANNEX A – REQUIREMENTS

We request that the contractor must be able to provide ALL the following services:

a. Globally recognized sets of Security Controls, related Guide Books and Compliance mappings to protect the organization from cyber-attacks;
b. Configurations Guidelines across at a minimum Amazon Web Services (AWS), Microsoft, Google, Oracle and IBM product families to safeguard departmental IT systems against cyber threats;
c. Resources and automated tools designed to measure compliance and identify vulnerabilities to secure the department;
d. Access resources for threat prevention, protection, response, and recovery for public sector organizations;
e. Provide an account-level starting point for configuring securely in the public cloud. These resources include identity and access management, logging and monitoring, networking, etc.;
f. Foundational guidance on AWS, Azure, Google Cloud Platform, Oracle Cloud and IBM Cloud;
g. Cloud Service Provider (CSP) product and service configuration guidance, including areas such as compute, databases, storage, and containers. Enable the selection of the applicable cloud services and configure them according to their environment.;
h. Hardened machine images with compliance mappings and security assessment report; and
i. Recommendations referenced to industry guidelines to inform the user of the guidance available from the CSP for both security and otherwise.

ESDC uses these services to:

1. Using the hardened server images, they harden and scan on a weekly hundreds of servers with new servers being added on a monthly basis. The hardened images are prepared ahead of time by Contractor for immediate consumption. Project teams usually complete the build design and start implementing with a turn around time of less than 2 weeks. These each of these hardened server images gets patched on average monthly and ESDC automatically applies these patches to these hundreds of servers.

2. Using the configuration guides and automated security scanning, ESDC project teams use the automated scanning to complete vulnerability scans done sometimes several times in a week near the end of the development lifecycle.

ANNEX B – RESPONSE REQUIREMENTS

The purpose of this Request for Information (RFI) is to obtain detailed information from vendors. ESDC has outlined below a list of questions and are requesting vendors to respond in detail, so that ESDC can compile information about subscription type of information on cyber threat prevention, protection, response, and recovery and provide benchmarks, scanning tools, guidelines and other related information on secure configurations related to secure cloud initiatives.

This RFI is not a commitment with respect to future purchases or contracts. In preparing their responses the Vendor community should refer to the Appendices as well as the questions below.

ESDC is asking the Vendor community to provide the following:

1. CORPORATE PROFILE

Each Vendor should provide the following information:

1) Company name, address, telephone & fax numbers and e-mail address.
2) Company contact name and telephone number.
3) 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.)
4) Identify how long your company has been working on providing information on cyber threat prevention, protection, response, and recovery and provide benchmarks, scanning tools, guidelines and other related information on secure configurations related to secure cloud initiatives.

2. QUESTIONS

ESDC is asking the Vendor community to respond to the questions below. If a question is not relevant to your Solution, please indicate that with an explanation regarding why the question is not relevant.

#	ESDC Question	Vendor Response
1.	Based on the services listed in the Annex A – Requirements (bullets a to i), cross identify which of the services you provide on cyber threat prevention, protection, response, and recovery and provide benchmarks, scanning tools, guidelines and other related information on secure configurations related to secure cloud initiatives. Include details on how you advise clients to secure an organization as a whole and how you advise clients to secure specific technology platforms and	

#	*ESDC Question*	*Vendor Response*
	the frequency by which you provide the tools. If possible, identify which specific technology platforms on which you provide advice noting that at a minimum AWS, Azure, Google Cloud Platform, Oracle Cloud and IBM Cloud are required.	
2.	Confirm that the services are provided as a subscription. If a vendor has more than one type of service or subscription, please provide a description for each subscription option.	
3.	Is there other related information provided by your subscription or alternative solutions that you feel would be of interest to ESDC for this requirement. If so, please describe.	
4.	Identify any clients who are currently using your services for an IT Security and Cybersecurity role at an organizational level. In particular, describe if any of them are in the public sector.	
5.	Identify how the information is provided to the user. Is it costed through a monthly or annual subscription?	
6.	Describe the pricing model for the subscription. Is there any limitation on the number of users?	
7.	Describe how benchmarks are created, who is involved and how they are provided to clients.	
8.	Describe if scanning tools are available to clients and can they be downloaded?	
9.	Describe how you provide hardened images to clients on secure, on-demand, scalable computing environments in the cloud and the method by which clients obtain this information.	
10.	Describe the support services provided to the users and identify the hours of coverage.	
11.	Confirm that the service provides compliance reports and provide a sample.	
12.	What is the average time for a client to deploy one of the deployment guidelines?	

3. ALTERNATIVE SUGGESTIONS

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