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 0B2 / Noyau 0B2
11 Laurier St.,/11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
RFI / National Cybercrime Solution

Solicitation No. - N° de l'invitation	Date
M7594-200151/A	2019-06-05
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
M7594-200151	PW-$$XL-126-35782
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
126xl.M7594-200151	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-06-21

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:	Buyer Id - Id de l'acheteur
Martyniuk, David	126xl
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 402-0570 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
David.martyniuk@tpsgc-pwgsc.gc.ca

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	Delivery Offered - Livraison proposée
See Herein	

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
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Canada

REQUEST FOR INFORMATION REGARDING A NATIONAL CYBERCRIME SOLUTION

TABLE OF CONTENTS

REQUEST FOR INFORMATION REGARDING
A NATIONAL CYBERCRIME SOLUTION
FOR
THE ROYAL CANADIAN MOUNTED POLICE (RCMP)

1) Background and Purpose of this Request for Information (RFI)

In 2015, the Minister of Public Safety and Emergency Preparedness lead "a review of existing measures to protect Canadians and our critical infrastructure from cyber threats". The review concluded that Canada needs a national mechanism to coordinate law enforcement operations against cybercriminals, and a national framework for Canadian citizens and businesses to report cybercrimes to police.

Currently, law enforcement responds to cybercrimes in isolation and on an incident-by-incident basis at the local level. It lacks the ability to connect the dots and assess the wider macro-economic and victim impacts of cybercrime.

The objective of this RFI is to request information from Industry that addresses the concise problem statement presented here, in a challenge format.

a. National Cybercrime Coordination Unit Mandate

Cybercrime is often under-reported as the reporting mechanisms in Canada are confusing for the Canadian public. The mandate of the National Cybercrime Coordination Unit is to:

- facilitate the coordination, synchronization and deconfliction of Canadian cybercrime investigations and collaboration with international partners;
- provide digital investigative advice and guidance to law enforcement agencies;
- produce actionable cybercrime intelligence for Canadian police; and
- operate a cybercrime victim reporting system for Canadian citizens and businesses.

b. The Current State

Canada lacks a national coordination centre for law enforcement cybercrime efforts. Currently, Canadian law enforcement agencies respond to cybercrimes in isolation and on an incident-by-incident basis at the local level; they lack the ability to connect the dots and assess the wider macro-economic and victim impact of cybercrime, and respond accordingly. This gap leads to inefficiencies and duplicative efforts. Cybercrime is often under-reported and there are many reporting mechanisms which are confusing for the public, businesses and cybercrime victims. Canada lacks a national mechanism dedicated to improving how businesses and the public report cybercrime incidents to law enforcement.

Towards achieving the target state, the RCMP is currently developing, as part of the National Cybercrime Solution, a public facing website that will allow Canadians citizens and businesses to report cybercrimes. This Cybercrime Reporting System is a component of the final NC3 Solution but is not included in the scope of this Request for Information.

c. The Target State

Canada wants to provide to Canadian citizens and the Canadian law enforcement community access to timely, adequate and integrated information for accurate and strategic decision making. The target solution must include business processes and workflows, information exchange and information workflows, categorization and assessment of information by business rules and analytics.

As a requirement of the target state, the cybercrime coordination unit requires access to a centralized structured and unstructured data repository for the secure storage and retrieval of digital information of various types, varying sizes, related metadata, allowing for growth of data without degrading performance.

RCMP law enforcement partners will also require access to a secure portal in order to seek, or provide information. The solution is expected to provide a service to partners that will identify Malware and that will act as a broker for such requests: receiving the malware sample, preparing a hash and determining whether the sample matches to an existing record. The target state solution is illustrated in appendix A.

A number of capabilities and business considerations are required across all aspects of the solution as follows:

- Capability to translate text from multiple languages with a high degree of accuracy into English and/or French is required. The system should be trainable to use specific terms and expressions common to criminal activities, in particular Cybercrime. Source document or file for the translation cannot be altered by the process.
- Voice recognition and transcription minimally in French and English is also required. Optionally, direct multilingual translation from multiple languages to English and/or French.
- For all modes of receipt of information, the system must maintain a copy of the source information, as well as any derived document or product to maintain traceability to the source.
- Complete Information Lifecycle Management including data management, permissions, protection, archiving, purge, etc. The lifecycle management must adhere to specified retention periods of the information being managed;
- Capability to support Artificial intelligence (AI) and Machine Learning (ML) based algorithms and methods in Big Data Processing and Analytics;
- Track and record, in a log file, the activities of all user(s) and the interactions of users, including the system. A non-alterable audit log of all relevant user and system activities must be created and retained.

The proposed capabilities must align, be scalable and allow for compatible integration with exiting RCMP internal technical systems and application.

2) Nature of Request for Information

This RFI is a consultation initiative by which the Royal Canadian Mounted Police (RCMP), hereafter referred to as Canada, is requesting Industry feedback on proven business and technical solutions, including lessons learned and best practices that will support Canada in satisfying the requirements for a National Cybercrime Solution. Following this RFI, Canada may use industry feedbacks to advance one or a series of Request for Proposals (RFPs) with the focus on industry's ability to deliver the solution.

This RFI is neither a call for tender nor a Request for Proposal (RFP). No agreement or contract will be entered into directly pursuant to 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 by Canada to issue a subsequent solicitation or award contract(s) for the work described herein.

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential firms 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 solicitations.

3) Response Costs

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

4) 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) and PWGSC 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) Follow-up Activity: Following the closing date, Canada may, in its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response. Canada may also at its discretion invite a Supplier(s) to present a demonstration of their solution in accordance with this RFI. The Contracting Authority will conduct the follow-up activity with any Supplier at its discretion. .

5) Contents of this RFI

This RFI also contains specific questions addressed to the industry:

Corporate Profile
1. Describe your corporate qualifications and expertise in the field of Cybersecurity. 2. Are your current business offerings aligned with the Government of Canada digital strategy providing Cloud services, Artificial Intelligence capabilities, etc.? 3. Has your company worked with other vendors towards an integrated enterprise solution in the past three years? If so, briefly describe the circumstances and results. 4. Describe your company's achievements with respect to data analytics in the past five years. 5. Describe your company background and experience in building structures, processes and environments that foster information sharing and collaboration.
Vendor Solution
6. Is your solution a Commercial-off-the-Shelf (COTS) application? 7. Does your solution have all the components described in this document and in Appendix A (Target State View)? If not, please explain the functional gaps. 8. If your solution does not have all the components described in this document, is your organization willing to engage other vendors in a joint venture to propose a solution that will meet all the requirements described in this document? 9. Have you implemented your solution within a federal, provincial or any other institution public or private agencies? 10. Does your solution currently have an Artificial Intelligence/Machine Language (AI/ML) functionality? 11. What other aspects/functionality would you recommend to add value to this solution? 12. Does your solution operate in both of Canada's official languages (English, French)? 13. How would the solution adapt to future technological and business requirements changes? What options does the vendor propose to address ongoing and evolving changes to business requirements? 14. Based on your experience, what are the current Cyber investigative methodologies? Which one would you recommend based on the understanding of our requirements? 15. Based on your experience, describe best practices related to Cyber investigation and reporting (DNS seizure / Domain seizure / Crypto currency seizure). 16. Describe the solution's future roadmap with expected release timelines.

Business and Training Materials

17. Based on your experience, what are the current data/information coordination/analysis methodologies? Which one would you recommend based on the understanding of our requirements?
18. Do you have training materials readily available for new users of your solution?
19. Based on your experience, describe best approach and practices related to data/information coordination/analysis training delivery.
20. Gamification of the learning process: describe your experience creating a virtual environment where people can learn and share best practices..

Technical Compliance

21. Will the hardware and software component of your solution use ISO standards, another form of standards, or will any parts/components be proprietary?
22. The RCMP requires a high degree of confidence in the users' identity by employing a strong 2-factor authentication method. How does your solution provide 2-factor authentication?
23. The RCMP must be able to remove its data, or copy its data from the solution in a non-proprietary and useable format at any time. How would your solution meet this requirement?
24. Is the software compatible with the industry leading technology (including but not limited to: operating systems, database systems, mobile devices, internet browsers)? Please provide minimum version requirement details.
25. How readily can your solution be deployed in a Cloud environment?
26. How and when have you deployed in a public Cloud environment? Which Cloud vendor's platform has your solution been deployed on?
27. Is the solution designed following enterprise architecture standard or any other industry's leading architecture framework?
28. Has the solution been designed to present a NIEM compliant interface for information exchange with external systems?

Questions for Cloud Implementation

29. Does the vendor's solution comply with Cloud services, Artificial Intelligence (AI), Machine Learning (ML) capabilities and the Government of Canada Digital Architectural Standards as described in: *https://www.canada.ca/en/government/publicservice/modernizing/government-canada-digital-standards.html*; and *https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/gc-earb-ceai/en/gc-earb.html*
30. The RCMP has a requirement to retain full ownership of all its business data. How would the vendor or solution meet this requirement?
31. The RCMP has a requirement to evaluate the performance, availability and security of its solutions using internal processes and tools and/or 3rd party tools. How would the vendor or solution meet this requirement?

32. The RCMP has a requirement for transparency of all security violations that affect RCMP services or data. How quickly and completely does the vendor report these violations?
33. The RCMP has a requirement to ensure all data resides within Canada data centres within the boundaries of Canadian Borders. How does you solution meet these requirements?
34. The RCMP requires that all vendor activity, involving RCMP data, be fully logged and auditable. It is further required that the vendor obtains written approval from the RCMP before accessing the data. Please explain how the solution monitors and tracks vendor activities.
35. The RCMP may want to use an IDaaS provider to provide a consistent external identity service. How would you meet this requirement?
36. The RCMP will require an audit (e.g., billing, usage, solution performance, availability, service interruption) of the services provided. What types of reports are available and how quickly can the reports be provided?
37. The RCMP has a requirement to have all data encrypted at rest and in transit. How does your solution meet these requirements?
38. The RCMP may want to use a Key Management Service for the storage and management of encryption keys. How would you meet this requirement?

6) Confidentiality of Supplier Responses

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 future solicitation or contract documents.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third-party or personal. 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.

7) Opportunity for an Information session

Canada may at its discretion hold an information session with Industry on this RFI. The date, time and location of the information session, if required, will be published at a later date. The information session if required, will provide interested vendors with an opportunity to seek clarifications on the objective and content of this RFI.

8) Vendor Demonstration

Canada may at its discretion hold demonstrations with Industry on this RFI. Vendors should express in writing their interest in providing to Canada a demonstration of their solution in response to this RFI. The vendors' demonstration of their solution will be done individually and the content will be kept confidential. The date, time and location of the vendor demonstrations will be scheduled by the contracting authority and communicated in writing to interested vendors.

Two scenarios that shall be used in the vendor demonstration are provided in the sections that follow. The objective is for vendors participating in the demo to demonstrate how their solution meets the business requirements as stated in those scenarios.

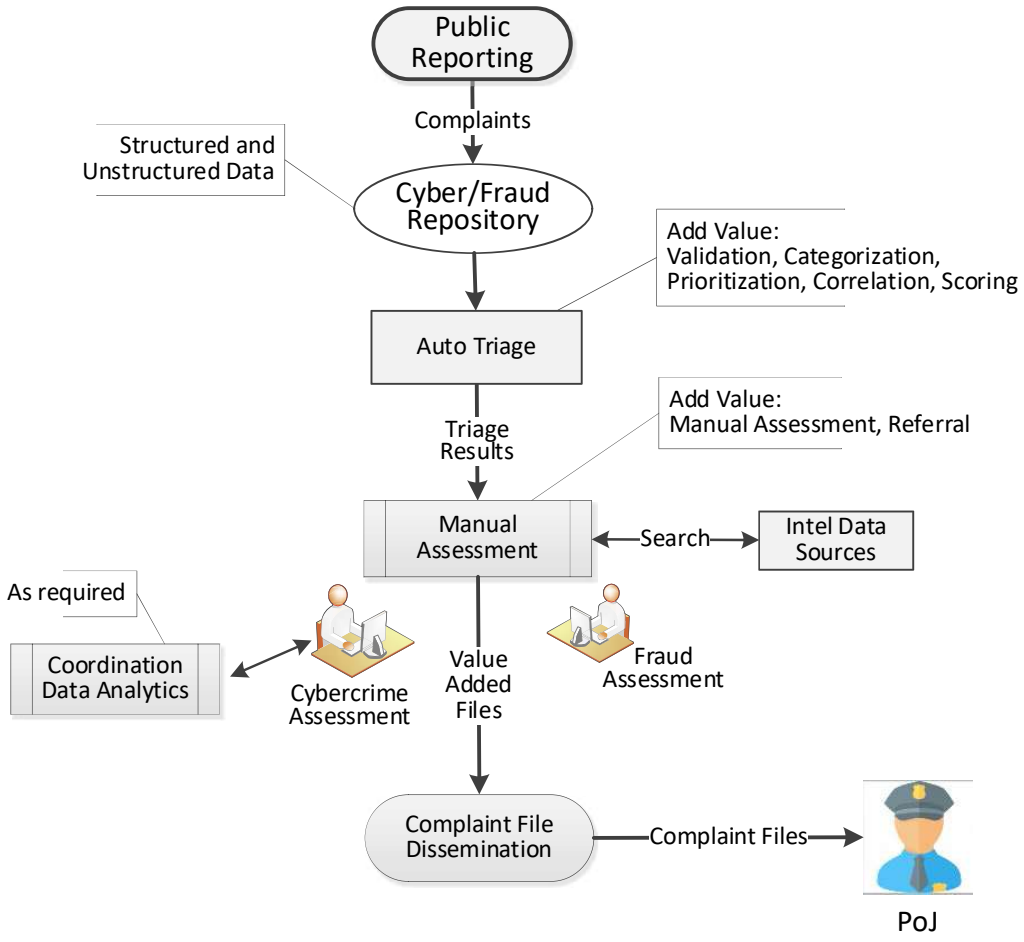
Scenario 1: Public Reporting

Public Reporting involves the capture of cybercrime and fraud reports from the public, ingestion of the reports into the Cyber Repository, Triage and Assessment of the reports and dissemination to Law Enforcement Partners for potential further investigation.

The solution will use a Triage process to analyse Complaint Files. Triage will determine whether the Complaint File has actionable status and apply a score to determine further processing. The Triage process may utilize Natural Language Processing to make inferences and extract data from text fields as well as Machine Learning to support advanced scoring algorithms. The Triage process is critical to prioritizing Complaint Files. Triage must be configurable to handle different types of data input as well as control the volumes requiring Manual Assessment.

Manual Assessment will further analyse and possibly add value to actionable Complaint Files prior to dissemination to Police of Jurisdiction.

The following diagram illustrates the Public Reporting concept:



Scenario 2: Receive Information/Query Submission

The solution will receive raw data, information and intelligence submissions or query requests from various domestic and international cybercrime partners. These submissions can be submitted for reasons that might include:

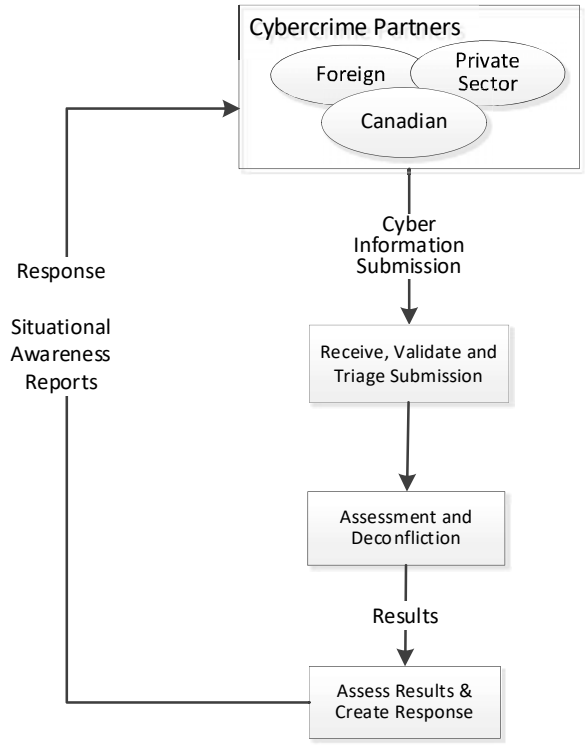
i) Query purposes – Are there any data holdings related to the information?

ii) Information only – Information is provided for cybercrime reference purposes

iii) Assessment and Response – Assess the provided information and return a response

The NC3 Unit will use the solution to log the submission, manage workflow, assess the submission, store cyber entities in the Cyber Repository, prepare the information for processing and perform any necessary query and deconfliction activities. The solution will also be used to develop and disseminate resulting Situational Awareness Reports.

The following diagram illustrates the process related to Information/Query submissions.



9) Format of Responses

a) 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.

b) 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.

c) **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.

d) **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.

e) **Number of Copies**: Canada requests that respondents submit 1 soft copy of their responses.

10) Enquiries and Submission of Supplier Responses

All enquires on this RFI should be directed to the Contracting Authority named below. Suppliers interested in providing a response should deliver it to the Contracting Authority identified above by the time and date indicated on page 1 of this document.

Contracting Authority: David Martyniuk
E-mail Address: David.Martyniuk@tpsgc-pwgsc.gc.ca
Telephone: 613-402-0570

APPENDIX A: TARGET STATE VIEW