Canada Revenue Agency | Agence du revenu du Canada

RETURN BIDS TO : - RETOURNER LES SOUMISSION À:

Canada Revenue Agency
Agence du revenu du Canada
See herein / Voir dans ce document

Proposal to: Canada Revenue Agency
We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein and/or attached hereto, the goods and/or services listed herein and on any attached sheets at the price(s) set out therefor.

Proposition à : l'Agence du revenu du Canada
Nous offrons par la présente de vendre à Sa Majesté la Reine du Chef du Canada, en conformité avec les conditions énoncées dans la présente incluses par référence dans la présente et/ou incluses par référence aux annexes jointes à la présente et ci-jointes, les biens et/ou services énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Bidder's Legal Name and Address - (ensure the Bidder's complete legal name is properly set out)
Raison sociale et adresse du Soumissionnaire - (s'assurer que le nom légal au complet du soumissionnaire est correctement indiqué)

_____

_____

_____

Bidder is required to identify below the name and title of the individual authorized to sign on behalf of the Bidder – Soumissionnaire doit identifier ci-bas le nom et le titre de la personne autorisée à signer au nom du soumissionnaire

_____
Name /Nom

_____
Title/Titre

_____
Signature

_____
Date (yyyy-mm-dd)/(aaaa-mm-jj)

(____)_____
Telephone No. – No de téléphone
(____)_____
Fax No. – No de télécopieur

_____
E-mail address – Adresse de courriel

AMENDMENT TO REQUEST FOR PROPOSAL / MODIFICATION DE DEMANDE DE PROPOSITION

Title – Sujet

Anonymous CRA internal fraud and misuse reporting lines

Solicitation No. – No de l'invitation	**Date (yyyy-mm-dd) (aaaa-mm-jj)**
1000318737/A	2015-01-08

Amendment No. - N° modif.

002

Solicitation closes – L'invitation prend fin on – le	**Time zone – Fuseau horaire**
2015-01-21 **(yyyy-mm-dd) (aaaa-mm-jj) at – à 2:00 P.M. / 14 h**	EST /HNE Eastern Standard Time/ Heure Normale de l'Est

Contracting Authority – Autorité contractante

Name – Nom Phuong Ly

Address – Adresse - See original document/ voir document original

E-mail address – Adresse de courriel – Phuong.Ly@cra-arc.gc.ca

Telephone No. – No de téléphone
(613) 957-3291

Fax No. – No de télécopieur
(613) 957-6655

Destination - Destination

See herein / Voir dans ce document

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT.

LE PRÉSENT DOCUMENT COMPORTE UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ.

SOLICITATION AMENDMENT # 002

This solicitation amendment is raised to:
1. **Address the following questions submitted during the solicitation period as per RFP; and**
2. **Amend the RFP.**

1. QUESTIONS AND ANSWERS

Q10. As the due date for responses is next week, and your responses may cause us to alter our responses, we'd love to get them as soon as possible. Or is it possible to receive a short extension for response submissions? Can the closing date be extended to Jan 31?

A10. CRA is not in agreement to extend the bid closing date to January 31, 2015. However, the bid closing has been changed to January 21, 2015. Refer to modification M3 below.

Q11. Would CRA accept an alternate pricing strategy versus monthly fixed fee?

A11. The CRA is requesting a firm all-inclusive monthly fixed rate so that all financial bid proposals can be evaluated consistently and fairly.

Q12. Can CRA provide us with number of submissions received in the last three years?

A12. As the CRA does not currently have any formal anonymous reporting system in place, we are not able to provide the number of submissions received.

Q13. Is CRA prepared to remove the requirement for the vendor to omit the Sources name and any personal information/identifiers from the report?

A13. Yes. The vendor, however, must provide warnings and reminders to the Source not to self-identify nor provide any personal information/identifiers. Please refer to modifications M4 and M5.

Q14. Within the list of mandatory requirements, our firm occasionally has more stringent processes than those requested by the CRA (for example, password renewals required more frequently than every 180 days; or the use of newer and/or more secure cryptographic encryption). If the CRA judges these to be more stringent, can you confirm that in those circumstances the requirement will be marked as 'met', as long as we state in our response that the basic requirement is met?

A14. Yes. The CRA will accept more stringent security configurations. As per "PART 3 - PROPOSAL PREPARATION INSTRUCTIONS" (page 10 of 60), the bidder must provide sufficient information demonstrating how they meet or exceed the stated requirement.

Q15. Within the list of mandatory requirements, our firm occasionally has processes that render a requirement non applicable (i.e. Protected B level information is not stored on miniature electronic storage devices). If the CRA judges these requirements to be non-applicable, can you confirm that in those circumstances, the requirement will be marked as 'met'?

A15. Yes. However, the vendor must still provide adequate explanation on why the requirement is not applicable or how the associated security risks are to be mitigated. The Bidder needs to provide sufficient detail in order for CRA to determine whether the Bidder meets CRA's requirement or not.

As per section 2.1 (Mandatory Requirements), all mandatory requirements must be met. In the example provided in the question, the bidder must identify how they manage the lifecycle of miniature electronic storage devices to ensure sensitive information is protected."

Q16 A. AC-2 a) Who does "the organization" refer to in this question (the CRA or the Bidder)? If a Bidder's administrative staff provides accounts and administrative support to CRA personnel designated by the CRA (in order to ensure the integrity of the system), is this acceptable to the CRA?

A16 A. "The organization" refers to the Bidder. The CRA requires the Bidder to provide sufficient information that indicates best practices for account management and account privileges are applied within the Bidder's organization. This includes management of all user accounts from internal IT administration accounts to CRA client accounts. The Bidder's suggestion above would provide some of the context for an acceptable response. Please see Supplemental Guidance under AC-2 at the following link {https://www.cse-cst.gc.ca/en/node/265/html/22840}.

Q16 B. b) If the Bidder's administrative staff set up user accounts for different classes of users based on their required functionality at the request of the client, is this considered acceptable to the CRA?

A16 B. This would address part of the requirement. The Bidder must also provide additional information that indicates best practices are followed for provisioning group membership to internal bidder employees. This includes access to different user groups or privileges (e.g. system admin, application admin, database management system (DBMS) admin, office staff, etc.)

Q16 C. j) By what criteria would the 30-day account review take place? What format should such a review follow?

A16 C. This requirement refers to the practice of reviewing all user accounts on a periodic basis to ensure user accounts have the authorized access privileges only, that unused accounts are properly suspended/deleted, etc. The CRA is seeking confirmation that the Bidder follows such practices for employee and client accounts. The criteria and format are up to each bidder organization based on their internal security processes.

Q17. AC-11 a) If there is a 15-minute timeout window in place for a Reporter submitting a report, and a 2-hour timeout window allowed for hotline agents as they are entering a report by telephone, is this acceptable to the CRA?

A17. From a security perspective, the proposed timeouts are acceptable. Refer to modification M5 below.

Q18. AU-2 a) If the Bidder maintains a log of database maintenance activities, and recycles this log every 7 days, is this acceptable to the CRA?

A18. The requirement states "(A) The organization must be capable of auditing the following events: system administrator and general user access to applications, database maintenance activities and system configuration changes." To meet this requirement the Bidder must have the capability to log system administrator and general user access to applications and system configuration changes, as well.

Further, requirement AU-11 states "(A) The organization retains audit records for 4 years plus the current year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements." Therefore, the retention period of 7 days is not sufficient to meet requirement AU-11.

Q19. AU-5 b) The Bidder has disk space limits set that send alerts so they may be addressed at several thresholds before any such failure would occur, negating the need for an audit system to shut down the information system or overwrite audit records. Is this acceptable to the CRA?

A19. Yes, as long as the proposed solution continues to respect the other auditing requirements on pages 51 and 52 under Audit and Accountability.

Q20. AU-11 a) Please specify the audit record retention lengths required for each different type of audit records.

A20. The required audit record retention lengths are 4 years plus the current year for each of the following:

- system administrator and general user access to applications

- database maintenance activities
- system configuration changes.

Q21. IA-5 e) Would the CRA consider prohibiting password reuse for 3 generations, instead of 10?

A21. Yes, the CRA will accept prohibiting password reuse for 3 generations. Refer to modification M5 below.

Q22. SC-12 and SC-13, the RFP calls for a section of the solution to be a website. This requires a HTTPS-based web service. The RFP documentation requires that the organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes as well as employing CSEC-approved cryptography to protect sensitive data. However, to secure a web-based service requires a different paradigm than is described in the documentation. For any HTTPS-based web service, certain cipher suites are required that combine the protocol, key exchange, digital signature algorithm, symmetric encryption algorithm and hash algorithm along with their respective bit strengths. In order to enable access for different browsers, it is necessary to support multiple such suites. Further, choosing the correct set of suites is key to providing a maximum level of security while at the same time enabling connections to a range of browsers. In the documentation provided, it is unclear which of these suites would be acceptable to the CRA. Please provide us with a listing of what the CRA considers approved cipher suites.

A22. The CRA will accept protocols and compatible cipher suites that meet the guidance provided in CSEC documents ITSB-60 (https://www.cse-cst.gc.ca/en/node/253/html/15204) and ITSA-11E (https://www.cse-cst.gc.ca/en/node/227/html/15164). The Bidder has the flexibility to adjust the list of supported protocols and cipher suites to maintain currency with mainstream browsers while adhering to the CSEC standards. For instance, widely used browsers like Internet Explorer, Chrome, Firefox, Safari, and Opera support TLS 1.0/1.1/1.2 as required by ITSB-60 and cipher suites using SHA-256 as identified in ITSA-11E. Refer to modification M5 below.

2. AMENDMENTS TO THE RFP

M3. On the first page of the RFP at Solicitation closes – L'invitation prend fin on – le :

Delete

2015-01-14

Insert

2015-01-21

M4. At Annex A-1: Business Requirements, Section 1.0 Task, subsection 1.1 Services Required

Delete

- Ensure the anonymity of the Source at all times (the Contractor must not record the Sources name at any time, even if provided);

Insert

- Ensure the anonymity of the Source by providing warnings and reminders to the Source not to provide any personal information/identifiers;

M5. At Annex A-3: Information Technology Security Requirements:

Delete:

AC-11	SESSION LOCK	(A) The information system prevents further access to the system by initiating a session lock after a CRA defined time period of inactivity or upon receiving a request from a user. (B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.

AND

AU-9	PROTECTION OF AUDIT INFORMATION	(A) The information system protects audit information and audit tools from unauthorized access, modification, and deletion (with the exception of omitting the Source's name and/or any identifying details).

AND

IA-5	AUTHENTICATOR MANAGEMENT	The information system, for password-based authentication: (a) Enforces minimum password complexity of uppercase and lower case letters, numbers and symbols (e.g. @, #, $, %); (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of 180 days or less; and (e) Prohibits password reuse for 10 generations.

AND

SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved (https://www.cse-cst.gc.ca/en/publication/itsa-11e) key management technology and processes.
SC-13	USE OF CRYPTOGRAPHY	The organization employs CSEC-approved (https://www.cse-cst.gc.ca/en/publication/itsa-11e) cryptography to protect sensitive data.

Insert:

AC-11	SESSION LOCK	(A) The information system prevents further access to the system by initiating a session lock after a maximum of 4 hours time period of inactivity or upon receiving a request from a user. (B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.

AND

AU-9	PROTECTION OF AUDIT INFORMATION	(A) The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

AND

IA-5	AUTHENTICATOR MANAGEMENT	The information system, for password-based authentication: (a) Enforces minimum password complexity of uppercase and lower case letters, numbers and symbols (e.g. @, #, $, %); (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of 180 days or less; and (e) Prohibits password reuse for 3 generations.

AND

SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes. The CRA will accept protocols and compatible cipher suites that meet the guidance provided in CSEC documents ITSB-60 (https://www.cse-cst.gc.ca/en/node/253/html/15204) and ITSA-11E (https://www.cse-cst.gc.ca/en/node/227/html/15164). The organization has the flexibility to adjust the list of supported protocols and cipher suites to maintain currency with mainstream browsers while adhering to the CSEC standards. For instance, widely used browsers like Internet Explorer, Chrome, Firefox, Safari, and Opera support TLS 1.0/1.1/1.2 as required by ITSB-60 and cipher suites using SHA-256 as identified in ITSA-11E.
SC-13	USE OF CRYPTOGRAPHY	The organization employs CSEC-approved cryptography to protect sensitive data. The CRA will accept protocols and compatible cipher suites that meet the guidance provided in CSEC documents ITSB-60 (https://www.cse-cst.gc.ca/en/node/253/html/15204) and ITSA-11E (https://www.cse-cst.gc.ca/en/node/227/html/15164). The organization has the flexibility to adjust the list of supported protocols and cipher suites to maintain currency with mainstream browsers while adhering to the CSEC standards. For instance, widely used browsers like Internet Explorer, Chrome, Firefox, Safari, and Opera support TLS 1.0/1.1/1.2 as required by ITSB-60 and cipher suites using SHA-256 as identified in ITSA-11E.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED