Correctional Service Canada Service correctionnel Canada

REQUEST FOR INFORMATION

THE CORRECTIONAL SERVICE OF CANADA

Lone worker protection systems for areas with and without cell coverage

TABLE OF CONTENTS

1.0 Background

1.1 Correctional Service Canada

Correctional Service Canada (CSC) is a Government of Canada agency within the Public Safety portfolio. This portfolio brings together key federal government organizations involved in public safety, including the Royal Canadian Mounted Police, the Parole Board of Canada, the Canada Border Services Agency, the Canadian Security Intelligence Service, and three review bodies.

CSC contributes to public safety through the custody and reintegration of offenders. More specifically, CSC is responsible for administering court-imposed sentences for offenders sentenced to two years or more. This includes both the custodial and community supervision of offenders with Long Term Supervision Orders (LTSOs) for periods of up to 10 years. CSC is currently responsible for approximately 14,400 offenders incarcerated in institutions and 8,700 offenders under supervision in the community.

CSC has a presence from coast to coast, in large urban centres with increasingly diverse populations, to more remote communities across the North. CSC manages institutions, treatment centres, Aboriginal healing lodges, community correctional centres, and parole offices. In addition, CSC has five regional headquarters that provide management and administrative support and serve as the delivery arm of CSC's programs and services.

1.2 Community Corrections

On any given day, Correctional Service of Canada staff supervises approximately 900 offenders in urban and rural communities across the Atlantic Region. As part of the reintegration process, offenders are released to the community under supervision.

1.3 Objectives of this Request for Information

As stated above, CSC is exploring options to provide additional safety measures in the form of lone working system protection for its community employees in the Atlantic provinces (New Brunswick, Prince-Edward-Island, Nova Scotia and Newfoundland and Labrador).

At this stage of the process, there are several operational requirements to which CSC would like to obtain more information from the industry, specifically the availability devices and/or APPs available to meet our needs. Those requirements are described in Section 3.0 below.

CSC has decided to issue a Request for Information (RFI) to industry, in order to elicit the expert opinions of private sector organizations specializing in the provision of relevant solutions.

2.0 The RFI Process

2.1 Nature of the RFI

This RFI is intended to:

- Invite industry experts and potential suppliers of relevant products and services to provide input as to potential solutions and approaches to meet CSC's requirements or to re-align CSC's expectations with industry capability, experience, and direction.
- Invite industry experts and potential suppliers to share their insights on any potential improvements to CSC's planned approach toward improving the security and safety of its staff.
- Invite potential suppliers to express the degree of interest that they may have in providing a solution to CSC.

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 may not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to the matters described herein.

2.2 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 should explain any assumptions they make in their responses.

There is no formal structure or format that a response to this RFI should meet. The Respondent should feel free to submit whatever information it feels would make a useful and relevant contribution to CSC's analysis of this project and the development of solicitation documents to procure products and/or services to fulfill its requirements.

CSC only requests that any submissions to this RFI cite the question appearing below (Section 5.0) to which the Respondent's information pertains. This will aid CSC personnel in the gathering and collating of submitted information addressing specific areas of the project.

2.3 Response Costs

CSC will not reimburse any Respondent for expenses incurred in responding to this RFI.

2.4 Treatment of Responses

2.4.1 Use of Responses

Responses will not be formally evaluated. However, the responses received may be used by CSC to develop or modify procurement strategies. CSC will review all responses received by the RFI closing date. CSC may, at its discretion, review responses received after the RFI closing date.

2.4.2 Review Team

A review team composed of representatives of CSC will review the responses. CSC 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.

2.4.3 Confidentiality

Respondents should mark any portions of their response that they consider proprietary or confidential. CSC will manage the responses in accordance with the Access to Information Act.

2.4.4 Follow-up Activity

CSC may, in its discretion, contact any Respondents to follow up with additional questions or for clarification of any aspect of a response. CSC may invite one, some, or all of the Respondents to present their submissions and/or perform a product demonstration for CSC. CSC is not obliged to invite any Respondents for this further exploration nor are any Respondents obliged to participate.

2.5 Enquiries

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

CSC Contact:	Chantal Goudreau
E-mail Address:	Chantal.Goudreau@csc-scc.gc.ca
Telephone:	506-851-6305
Facsimile:	506-851-3305

2.6 Submission of Responses

Suppliers interested in providing a response should deliver it to the CSC contact identified above by 14:00 ADT on August 18th, 2017. Each Respondent is solely responsible for ensuring its response is delivered on time to the correct location.

3.0 Work Alone System Protection Requirements

The following is a list of high-level requirements CSC has identified for a work alone system protection. This list was developed through a preliminary examination of the factors driving the need for a solution based on the current working conditions and staff safety protocol for staff who conduct business alone away from the office and in the community.

1. Technical device

Provide CSC Atlantic Region with lone working system protection for two types of Blackberry Smart phones, i.e. Blackberry 10 and Blackberry Bold (9900, 9780). These devices could be changed to another brand of cell phone in the future; therefore, it would be important to note what type of phones your system can function with.

2. Administrative service

Provide the ability to modify the current users of the APP or device as needed, e.g. add a new user when required and when need be modify the contact protocol as necessary.

3. Information Management

Provide CSC with current information as relayed by the CSC employee when he/she has shared the location (physical address of a visit and the names of persons to be visited) as well as the duration of the community visit.

4.0 Security Clearance Requirements

4.1 Anticipated Security Clearance Requirements- Request for Proposal (RFP)

A security clearance is a certification that is granted by the Canadian Security Program (CSP) of PSPC.
If the process continues, security requirements will be set out in the Draft Request for Proposal (RFP) and the final RFP. As the requirement is refined, Canada will finalize the supplier security profile requirements; however, Canada currently anticipates that Bidders will require, at minimum, the following security clearances at the RFP stage:

a) Reliability Clearance from CSP for any Bidder who will have access to any information that is sensitive and/or proprietary to Canada or to a third party (herein-after referred to as “Sensitive Information”);

b) Document Safeguarding Capability (DSC) from the CSP for the facility at which the Bidder intends to use and store Protected Information; and

c) Information Technology Security capability vetted by CSP for the facility at which the Bidder intends to use and store Sensitive Information, in order for the Bidder to be able to process, store or transmit Protected Information electronically.

Suppliers should expect that personnel assigned to participate in the work will be required to be security cleared to the level of Reliability at minimum.

Canada currently expects that any resulting contract may require some or all of the following contractual obligations and restrictions:

a) Individuals employed by the Contractor, who are required to work with drawings/documents or visit some of the government sites, must have a Reliability clearance;

b) All persons performing Contractor duties under the contract must have a security clearance at the appropriate level. Accordingly, the Contractor must ensure that appropriate personnel have the required security clearance levels, and the Contractor must ensure that security clearances of its personnel are processed in advance to ensure that they are in place when required; and

c) Security requirements and protocols will exist to ensure that Sensitive Information and ownership in the control of the Contractor, the facility, and the initiative are not acquired by any person who does not have appropriate security clearances as a result of any assignment, transfer, or disposition by the Contractor, change in control of the Contractor, exercise of remedies by lenders, or otherwise.

4.2 Canadian Industrial Security Directorate Security Process

Security clearances (issued by CSP) will allow Contractors to work on Government of Canada premises and have access to confidential or Protected Information if/as required. The Government of Canada Security Policy requires that individuals undergo a personnel-screening process if their duties or tasks necessitate access to Classified/Protected information and assets.

Suppliers must be sponsored by a representative from Canada in order to start the process of obtaining or upgrading a security clearance directly in support of the initiative.

Suppliers that do not currently have personnel and organization security clearances through the Canadian federal government should refer to the Contract Security Program (CSP) of Public Services and Procurement Canada website.

Early submission of all applications for security clearances is strongly encouraged. Suppliers are strongly encouraged to submit applications for security clearances for all key individuals and any other persons who may be required during the implementation phases to have access to Sensitive Information and/or access to secured sites. Procurements will not be delayed in order to provide time for suppliers to obtain required security clearances.

4.3 Anticipated Data Sovereignty

The protection of information, from a privacy and security perspective, is core to the integrity of government programs, which underpins confidence in Canada. All information managed by Canada requires protection, including information published publicly in order to appropriately protect the confidentiality, integrity and availability of the information. The information up to and including “Protected B” may be shared while using the work alone system, and it is incumbent that the work incorporates the appropriate controls in order to safeguard the interests of Canada and those of its partners to this level of security. No information above Protected B will be shared by community employees in the course of their duties.

Furthermore, security controls, which ensure the confidentiality, integrity and availability of the work, are imperative requirements for the work alone monitoring system, as Canadians expect Canada to take all appropriate measures to protect personal and Sensitive Information.

Therefore, the required services and/or infrastructure are anticipated to be established within the political and geographic boundaries of the Atlantic Region in Canada. Stringent contractual and technical measures must be put in place to ensure that government information is secured at all times, at rest and in motion, through encryption protection and is only accessed by those authorized to access the infrastructure for those purposes approved by Canada.

4.4 Data Privacy and Information Security

All data must be managed in accordance with Canadian Security Establishment “IT Security Risk Management Life Cycle Approach” (i.e. CSE ITSG-33). It is anticipated that PB-M-M Security Control Profile will be applicable for this requirement.

Canada will require the service provider to establish and maintain a data privacy and information security program, including physical, technical, administrative, and organizational safeguards that is designed to:

a) Ensure the security and confidentiality of Canada’s Data;

b) Protect against any anticipated threats or hazards to the security or integrity of Canada’s Data;

c) Protect against unauthorized disclosure, access to, or use of Canada’s Data;

d) Ensure the proper disposal of Canada’s Data; and

e) Ensure that all employees, agents, and subcontractors of the Contractor, if any, comply with all of the foregoing.

4.5 Supply Threats to the Government of Canada

In addition to the threat of cyber-attack, there is a growing awareness of the risks posed by potentially vulnerable or shared technologies that may be entering the GC communications networks and IT infrastructure through the supply chain. The service provider, when and wherever applicable, will be required to provide the GC with a list of all hardware and software manufacturers and suppliers proposed to be used in the IT Infrastructure and services in advance of contracting with them. Canada reserves the right to reject a hardware or software manufacturer and/or supplier for security and/or business stability reasons.
The service provider will be required to abide by the Technology Supply Chain Guidelines (TSCG).

5.0 Questions to Industry

(AREAS WITH CELL COVERAGE)

The Atlantic District Office of Correctional Service of Canada has a need for information relating to lone monitoring systems that work in areas with cell coverage. Furthermore, the service required must work with all cell phone types. The following questions are provided for the sole purpose of acquiring information on the various types of services offered and available for work alone systems which could provide monitoring of approximately 110 CSC employees conducting business in the Atlantic region from Monday to Friday between the hours of 07:00 hours to 18:00 hours (Newfoundland Standard Time Zone and Atlantic Time Zone); they would be visiting offenders and/or their family, friends, employers, acquaintances in order to assess the offender's compliance with his/her release conditions. A lone monitoring system is required to ensure that each employee can signal an urgent matter, request help, or simply check-in to indicate that he/she is safe while doing his/her job.

Please note: A response to these questions does not indicate that you or your company has entered into a contractual agreement or that it has any influence on future solicitation for contracting with Corrections Canada; this exercise is simply to gather information on what the industry has to offer for work alone system protection for areas with cell coverage.

1. How does your device/APP become activated to commence monitoring?

2. How can a CSC employee indicate an address they are visiting and scheduled time for which the monitoring system would keep this information?

3. Is there a capacity to change a schedule after an employee has logged a visit? How would this be done?

4. Does the system work inside buildings?

5. Does the system use text, an APP or other to conduct monitoring?

6. Is there a means to maintain a regular (e.g. hourly) check-in with the employee between the time the visit begins and ends while he/she is conducting business? How would you propose monitoring a high risk situation? (e.g. hourly calls)

7. Are there components of your device/APP/software which provide no-motion, man-down, shake for panic, or a request for help detection system? Please elaborate which and how each would work.

8. How does an employee advise that he/she is in distress?

9. How would the CSC employee advise that the monitoring period has ended?

10. Can you provide the cellular devices and models that this APP will work with?

11. Do you have administrators who input information for emergency contact protocol? Please provide a description of how this process is completed.

12. How is the billing calculated, i.e. do you charge per call or per user?

13. If your company were to offer services for 110 employees, would the cost associated to a year's service be (before tax):

    A. $1.00 - $9,999.99
    B. $10,000.00 - $ 19,999.99
    C. $20,000.00 - $29,999.99
    D. $30,000.00 - $39,999.99
    E. $40,000.00 +

14. Are there any potential additional fees with the provision of this service that is above and beyond the fixed cost? Please elaborate on how this is calculated.

15. How would you propose to offer the service of lone worker monitoring to Correctional Service of Canada (Atlantic Provinces: New Brunswick, Prince-Edward-Island, Nova Scotia, and Newfoundland and Labrador)?

16. Would you be able to offer services in both official languages?

17. Do you have any additional comments/information to provide CSC?

(FOR AREAS WITHOUT CELL COVERAGE)

The Atlantic District Office of Correctional Service of Canada has a need for information relating to lone monitoring systems that work in areas with NO cell coverage. The following questions are provided for the sole purpose of acquiring information on the various types of available technology, which could provide monitoring of CSC employees conducting business in the community in the Atlantic region from Monday to Friday between the hours of 0700 hours to 1800 hours (Newfoundland Standard Time Zone and Atlantic Time Zone); they (CSC employees) would be visiting offenders and/or their family, friends, employers, acquaintances in order to assess the offender's compliance with his/her release conditions. Therefore, a lone monitoring system is required to ensure that each employee can signal an urgent matter, request help, or simply check-in to indicate that he/she is safe and secure in areas that do not have cell reception.

Please note: A response to these questions does not indicate that you or your company has entered into a contractual agreement or that it has any influence on future solicitation for contracting with Correctional Service of Canada; this exercise is simply to gather information on what the industry has to offer for work alone system protection for areas without cell coverage.

1. How does your device become activated to commence monitoring in an area with no cell coverage?

2. How can a CSC employee indicate an address that he/she is visiting and for which the monitoring system would keep this information?

3. Is there a means to maintain a regular (e.g. hourly) check-in with the employee between the time the visit begins and ends while he/she is conducting business? How would you propose monitoring a high risk situation? (e.g. hourly calls)

4. Are there components of your device/APP/Software or Hardware which provide no-motion, man-down, shake for panic, or request for help detection features? Please provide a description of each system that is available.

5. How does an employee advise that he/she is in distress?

6. How does the escalation system work if there is no response?

7. How would the CSC employee advise that the monitoring period has ended?

8. How can you assure CSC that the device will provide monitoring while the employee is inside a building in areas where there is no cell coverage?

9. If your company were to offer services for 35 devices, would the cost associated to a year's service be (before tax):

   A. $1.00 - $9,999.99
   B. $10,000.00 - $ 19,999.99
   C. $20,000.00 - $29,999.99
   D. $30,000.00 - $39,999.99
   E. $40,000.00 +

10. Are there any potential additional fees with the provision of this service that is above and beyond the fixed cost? Please elaborate on how this is calculated.

11. Would you be able to offer services in both official languages?

12. How would you propose offering the service of lone worker monitoring to Correctional Service of Canada in the Atlantic Provinces: New Brunswick, Prince-Edward-Island, Nova Scotia, Newfoundland and Labrador for CSC employees who work in the community and have NO cell coverage?

13. Do you have additional comments or suggestions to offer?

COMBINED COVERAGE

1. Would you be able to provide service for both cell coverage and no cell coverage? How?

Note: *All financial details from Respondents will be treated as proprietary and confidential information if the Respondent makes a declaration of confidentiality in its submission.*

6.0 Useful Links

Corrections and Conditional Release Act Act (Justice Canada) :
http://laws-lois.justice.gc.ca/eng/acts/C-44.6/

Official Languages Act (Justice Canada):
http://laws-lois.justice.gc.ca/eng/acts/O-3.01/

Personal Information Protection and Electronic Documents Act (Justice Canada) :
http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Access to Information and Privacy (Government of Canada):
http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/index-eng.asp

Profile of Information Technology (IT) Services (Treasury Board of Canada Secretariat):
http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/profil/profiltb-eng.asp

Government of Canada buying and selling legislation and regulations (Public Services and Procurement Canada):
https://buyandsell.gc.ca/policy-and-guidelines/Policy-and-Legal-Framework/Statutes-and-Regulations

Security requirements for contracting with the Government of Canada (Public Services and Procurement Canada):
http://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

7.0 Links to the Government of Canada's Web/Application Standard

Standard on Web Accessibility:
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

Web Content Accessibility Guidelines (WCAG) 2.0:
http://www.w3.org/TR/WCAG20/

Web Experience Toolkit:
http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/ws-nw/wet-boew-eng.asp

Standard on Web Usability:
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227

Standard on Web Interoperability :
http://www.tbs-sct.gc.ca/ws-nw/wi-iw/index-eng.asp

Standard on Optimizing Websites and Applications for Mobile Devices:
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27088