Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Public Works and Government Services Canada
Telus Plaza North/Plaza Telus Nord
10025 Jasper Ave./10025 ave. Jaspe
5th floor/5e étage
Edmonton
Alberta
T5J 1S6
Bid Fax: (780) 497-3510

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Building & Personnel Security Sys

Solicitation No. - N° de l'invitation EW479-121057/A	**Date** 2012-05-08
Client Reference No. - N° de référence du client EW479-121057	**GETS Ref. No. - N° de réf. de SEAG** PW-$EDM-183-9410
File No. - N° de dossier EDM-1-34243 (183)	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2012-06-18

Time Zone
Fuseau horaire
Mountain Daylight Saving Time MDT

F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☑

Address Enquiries to: - Adresser toutes questions à: Taylor, Ian	**Buyer Id - Id de l'acheteur** edm023
Telephone No. - N° de téléphone (780) 497-3621 ( )	**FAX No. - N° de FAX** (780) 497-3510

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA
TELUS PLAZA N.5TH FL.
10025 JASPER AVE
EDMONTON
Alberta
T5J1S6
Canada

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 See Herein	**Delivery Offered - Livraison proposée**

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
Public Works and Government Services Canada
Telus Plaza North/Plaza Telus Nord
10025 Jasper Ave./10025 ave Jasper
5th floor/5e étage
Edmonton
Alberta
T5J 1S6

Canada

PART A - BACKGROUND

All Government Department and Agency offices are located in various types of establishments throughout Canada. While these offices have established building security, PWGSC is interested in exploring alternatives to safely secure these work environments as Canada has a requirement to safeguard all of its employees, assets and information.

Essential to the security plan and design of the work environment is the implementation of appropriate measures to deter, detect, delay and deny an attack on the property or persons employed within.

Public Works and Government Services Canada (PWGSC) is requesting information about various security solutions for government buildings and office places.

PWGSC is currently exploring the options of three different types of security features:

1. Building Access Systems;
2. Intrusion Alarm Systems;
3. Panic Alarm Systems.

OBJECTIVES

The objective of this Request for Information (RFI) is to solicit comments and suggestions from industry regarding particular requirements and challenges identified in the establishment of a building security Standing Offer (SO).

PART B – MODALITIES

In order to facilitate the management of comments and suggestions from interested parties, it is important that the following modalities be respected.

1. Identification of Information Provider

   All parties wishing to respond to this RFI should clearly identify themselves. At a minimum, the following information should be provided:

Name / Corporate name:	
Postal address:	
Name of contact person:	
Telephone number:	
Email address	
Geographic areas able to provide service:	
What areas of security can be provided:	

2. Format

   Except for comments and suggestions that are general in nature, the comments and suggestions should be clearly linked to a paragraph number and the specific issue as presented in Part C XXX. Interested parties should clearly formulate their comments and recommendations and substantiate the reasons why they consider these specific comments and suggestions should be considered.

3. General Information

   The material in this Request for Information (RFI) package is for the solicitation of interest and feedback only. Potential bidders are encouraged to indicate their level of interest by responding to this RFI with their comments using the questions raised in the RFI package, Part C – Requested Information.

   This RFI is NOT an invitation to submit proposals and no contract will be entered into as a result of this RFI. PWGSC could however take into consideration some of the comments and suggestions raised in the scope of this RFI in the refinement of the formulation of a future requirement. Comments and suggestions received could also be taken into consideration in the preparation of the Request for Standing Offer (RFSO) documents to be finalised by PWGSC.

   The publication of this RFI does not constitute in any way an obligation on the part of PWGSC and the Government of Canada to issue one or any number of Requests for Standing Offers for Building and Personnel Security Services.

The formulation of comments and suggestions by potential bidders will not constitute in any way an obligation on the part of PWGSC and the Government of Canada to contract with the bidder who formulated the comments and suggestions.

Neither PWGSC nor the Government of Canada will have any obligation to take into consideration those comments and suggestions from potential bidders. PWGSC will not publish a report outlining the comments and suggestions and will not communicate with potential bidders to inform them of PWGSC's decisions nor to explain its decisions following the comments and suggestions received.

Potential bidders who wish to formulate comments and suggestions in the scope of this RFI should take note that comments and suggestions must be provided on a courtesy basis and that neither PWGSC nor the Government of Canada shall indemnify the potential bidders for the time and expenses incurred for the examination of the documents nor for the preparation of the comments and suggestions.

4. Clarification

PWGSC may require clarification of written responses received and/or comments received as a result of the responses to this RFI. If required, any clarification will be requested by the Contact identified below after the closing date of the RFI. Requests for clarification will be submitted in writing (by facsimile or e-mail) and a response will be requested within five (5) working days of transmission of the clarification questions. PWGSC will not provide any guidance on how to prepare the responses or of any acceptable response strategy.

5. Closing Date

Responses to this RFI will be accepted until 02:00 PM Mountain Daylight Savings time (MDT) on June 30, 2012.
Responses are to be submitted in writing by mail, facsimile or e-mail to the identified Senior Contracts Officer below:

Name:	Alex Tikhonovitch
Title:	Supply Specialist Public Works and Government Services Canada Acquisitions Branch
Directorate:	Western Region
Address:	5th Floor, Telus Plaza North, 10025 Jasper Avenue, Edmonton, AB T5J 1S6
Telephone:	780-497-3541
Facsimile:	780-497-3510
E-mail address:	Alex.Tikhonovitch@pwgsc-tpsgc.gc.ca

PART C - REQUESTED INFORMATION

1. While the focus of this RFI is based on the following systems, are there other types of systems that can be used to enhance building and personnel security?
    1. Building Access Systems;
    2. Intrusion Alarm Systems;
    3. Panic Alarm Systems;
    4. _____;
    5. _____.

2. Are there any building codes that systems are installed to? Is the equipment manufactured to any industry standards? (ex. CSA, ASME, etc…)
3. What sort of monitoring services are available for each of the types of systems? Can they be monitored by the end user centrally, locally or by a service provider?
4. Are there any compatibility concerns that need to be addressed? Can the systems work independently of each other or can they work in tandem?
5. In some situations, a building may already have a general system installed. If the end user requires their own access system to be installed in their area, will the new system have to be compatible with the previous system or will it be able to operate independently?
6. What is your process in assessing a building's requirements for security systems? Are there basic questions that are asked of the end user? Are floor plans (drawings) needed?
7. What process do you have to evaluate the current safeguards and vulnerabilities?
8. When you see a requirement, what information are you looking for? How specific should a requirement be?
9. What is needed from the end user for you to make a proper quote?
10. What information is provided in your quote?
11. For systems that are being monitored by a service provider, who is the owner of the equipment on site?
12. Are there any concerns with Intellectual Property in relation to any of these systems?
13. What is the warranty on the products and work once installed?
14. Should there be any issues or concerns that arise during the course of the work, how are these addressed?
15. What sort of maintenance is required on each of these systems?
16. What geographical locations would you be able to support? Would you be able to provide goods and/or services locally, to various local regions, provinces, or nationally?
17. What training is provided on the systems, and who provides it?
18. What options are provided?
19. Are recommendations provided for door types and locking hardware in support of the systems?
20. Is the company able and willing to obtain federal security clearance, if not already in place?

The following pages contain examples of what may be asked for in relation to the different systems. Comments and suggestions are welcome.

Building Access System

Devices that assist in the physical security of the building/facility such as closed circuit television (CCTV) surveillance systems, intrusion detection and alarm systems, electronic access control systems, radio systems, etc. Includes remote central or direct control of security systems, equipment or monitoring devices interfaced with panels, field sensors, relays including all interconnecting wiring, cabling, piping and conduit. Includes power systems dedicated to these systems. Does NOT include tenant supplied/responsible equipment protecting Government assets in Government tenant reception, operational and restricted zones.

CARD ACCESS SYSTEM

System Requirements

The Card Access System will include the following components:

1. **System:**
   a. Must be modular design to support expansion modules;
   b. In off-line mode, the access controller should retain a minimum of 300 transactions on memory and should automatically upload to the host PC when communications resume;
   c. Each door equipped with a card reader is to be supervised through the control unit;
   d. An alert will be triggered on a door held in an open state longer than 15 seconds. The alarm is required to show on the system board and identify the issue but no audible alarm is required;
   e. Door supervision will require the use of magnetic door contacts;
   f. Power backup is to be provided for local readers/strikes/controllers. ACU must be equipped with a battery charger and back-up batteries capable of operating the ACU for up to 24 hours;
   g. The ACU enclosure must have a monitored tamper switch. Status is to be reported to host PC;
   h. Power surge protection is to be provided for critical system components.
2. **Card Readers:**

   a. Proximity card readers are required and are to be wall mounted (unless otherwise required);

   b. Failure of any of the controllers must not affect the operation of more than two card readers;
   c. The card reader is to be supervised by the access controller to automatically report cable breaks;
   d. Card Readers must have internal memory allowing access transaction retention for no less than 24 hours after a power interruption occurs.
3. **Electrical Door strikes will have the following features:**

   a. For use with bored locks, mortise locks or mortise exit devices having a 1/2," or 5/8" throw dead latch bolt.

4. **Other hardware considerations:**

   a. Doors equipped with proximity card readers will also be equipped with a local alarm sounder;

   b. Backup power supply capable of supply for 24 hours after power interruption and power surge protection must be provided for door strikes and card readers;
   c. Perimeter doors equipped with card readers will also have a key override feature;
   d. All hardware and installation must comply with fire and national building code regulations.

5. Considerations for the Card Access Management System:

a. The central card access control management system will support day to day administration/management of the site card access systems;

b. End user will have the responsibility to manage the card access management system from a remote location through their network;
c. The contractor will provide the software to operate the card access system on a computer to be supplied by the end user. The system will operate through a static IP on the internal network;
d. The access control management system is to be located on-site in a LAN Room;
e. The access control management system must be equipped with a data back-up system.

6. Cards and programming

a. 250 of access cards must be provided;
b. The contractor will pre-program cards in accordance to a list of approved card holders to be supplied by the end user.

7. Training:

a. The contractor is required to provide full training to up to 10 identified personnel on the operation of the card access system and the administration/management of the card access management system.

8. Warranty and Maintenance:

a. The card access system is to have a one (1) year warranty period on all parts, labour and maintenance from date of completed installation. Maintenance costs not to commence until the start of the second year;

b. The contractor must respond to non-critical system failure service calls within 24 hours of notification. For maintenance purposes, a non-critical system failure refers to any system deficiency requiring maintenance;
c. For critical system failure service calls, response must be provided within four (4) hours of notification. For maintenance purposes, a critical system failure refers to a system failure that would prevent central monitoring of the facility.

9. Reporting:

a. The access card management system must be capable of producing custom access control reports.

10. Installations:

a. All work awarded to a contractor must be completed without interrupting service.;

b. Commissionaires will be arranged (if needed) by the end user to monitor contractors and secure areas where work will be done.

PANIC ALARM SYSTEM

System Requirements

1. Supply and install fixed panic buttons in the identified areas:
   a. XXX.

2. Panic buttons shall be firmly mounted under the identified desks, out of view of clients, and shall be easily accessible.

3. To prevent false alarms, the buttons shall be protected by a housing into which the agent must place his or her finger in order to activate the alarm. Palm buttons are to be wall mounted and positioned in a manner which will allow activation during egress.

4. The signal is captured by a receiver mounted in the ceiling of each zone and linked to red, non flashing lights over the doors as well as the central alarm. Refer to section 12
   a. Note: Strobe lighting, in consultation with RCMP and health and safety, is not acceptable as it may trigger seizures in those individuals with photosensitive epilepsy. Audible sound, to draw attention to the area, in conjunction with a red non-flashing light is recommended.

5. The alarm shall stay on until the problem is resolved.

6. The monitoring station is to be installed in an area which is staffed throughout normal working hours.

7. A total of 20 mobile panic buttons (lanyard style) shall be supplied for employees who have direct physical contact with the public/clients.

8. The Contractor must submit a plan of the premises showing the location of the fixed panic buttons and identifying the corresponding rooms.

9. Location and installation of alerts. Alerts are to be equipped with battery back-up systems to ensure their functionality should a power failure occur for up to 12 hours.

10. The Contractor guarantees all materials, equipment and programming for a minimum of one year from the date on which installation is accepted.

11. The Contractor shall, during the guarantee period effectively and diligently resolve any problems within twenty four hours of being notified of a failure.

12. The manufacturer shall train the employees designated by the security representative. The manufacturer shall provide a qualified technician to train the designated employees on how to use the system.

13. After final acceptance of the work, the Contractor shall provide the following documents as required by the specifications:
    a. as-built drawings;
    b. the operating and maintenance manual.

14. It is the responsibility of local management to test the panic alarm system on a regular basis.

INTRUSION ALARM SYSTEM

Systems Requirements:

1. The intrusion alarm system shall meet the requirements of: Underwriters Laboratories Canada (ULC), Canadian Standards Association (CSA), municipal authorities and the National Building Code.
2. The intrusion alarm system shall have a module linking all of the components and shall be equipped with a digital device to relay signals to the central monitoring station through a telephone line. An alarm panel with zones and a keypad shall be installed in the building, and a plan (AutoCAD) showing the zones shall be provided to PWGSC and/or the occupant.
3. Supply and install near the entrance a smart digital keypad, with delayed entry/exit, for programming the system.
4. The system shall cover all useable areas of the premises.
5. Every cabinet or closet, housing electrical or mechanical systems, shall have a monitored tamper-proof switch.
6. Supply and install magnetic door contacts on all perimeter doors. Where possible, the contacts shall be set in.
   a. Hermetically sealed;
   b. Flush mounted in interior of door frame with magnet in the head of the door;
   c. SPDT contacts;
   d. Adjustable gap, suitable for metal doors; and
   e. Flexible conduit raceway connection supplied with all mounting hardware
7. Supply and install ULC-certified dual-technology (breakage and impact) glass break sensors near all windows that can be accessed from outside (ground floor, terraces, etc.).
8. Supply and install wide-angle and 360° passive infrared motion sensors in central areas and strategic locations.
   a. Mounted on an environmental enclosure, wall or ceiling mounted;
   b. Aimed at the intrusion protection area to be covered;
   c. Suitable for wet and extreme temperature environment (-18oC to 50oC);
   d. All motion detection equipment shall incorporate anti-tamper switches, which will be on a 24-hour loop;
   e. System is to be monitored during silent hours (excluding tamper switches) and is to annunciate at the monitoring site;
   f. Motion test light to be disabled after installation;
9. The chosen alarm system shall be capable of providing a personalized access code for every user (Maximum of 50).
10. The system shall be connected to an emergency power supply capable of running the system for 12 hours in the event of a power failure.
11. The monitoring station shall be capable of contacting the end user representative if the system is not armed and arming the system remotely.
12. Provide and install two 30 watt sirens, (as per floor plan or site contact) to be enclosed in a weather resistant enclosure complete with tamper switches. Sirens to provide local audible warning of 130db minimum and conform to local by-law restrictions. Sirens are to ring audible for a minimum of five (5) minutes.
13. The burglary control panel must have the following features:
    a. LCD keypad (2 line, 32 alpha-numeric character display);
    b. 16 programmable zones (expandable to 128);
    c. 128 user codes;
    d. 512 event buffer;
    e. telephone line supervision;
    f. siren circuit supervision;

g. upload/download support;
h. multiple keypad support;
i. built in digital communicator;
j. English-language text;
k. full battery standby.

14. The system must be capable of auto-arming based on time of day.
15. The system must be capable of auto-disarming based on time of day.
16. The contractor is to arrange Central Monitoring Services.
17. The end user will be responsible for installing the required jack to interface with the control panel.
18. The monitoring agency is responsible for producing regularly monthly reports (electronic) on system activity.

19. Response Procedures are to be provided to the end user and are to include:
    a. When a notice of intrusion is received a mobile patrol is to be dispatched to the premises. Upon arrival they are to do a perimeter check to look for signs of entry. If signs of entry are detected, then local police and the local office contact are to be contacted. The local office contact will be advised that Police are on their way. The mobile patrol person(s) are to remain on-site until they are released by either police or by the departmental contact;
    b. If signs of entry are not detected, then the mobile patrol will provide a written report to the end user.
20. In case of a false alarm, the contractor agrees to pay all charges arising from response activity by law enforcement agencies. The end user will reimburse those charges at cost. Response charges for false alarms occurring as a result of system failure will be the responsibility of the contractor.
21. The contractor is to arrange for on-site emergency alarm response to the end user’s premises as dictated by the Central Monitoring Station.
22. The contractor is required to provide full training to up to 10 identified personnel on the operation of the intrusion alarm system and the administration/management of the system.
23. Warranty and Maintenance:
    a. The card access system is to have a one (1) year warranty period on all parts, labour and maintenance from date of completed installation. Maintenance costs not to commence until the start of the second year. Warranty periods beyond a year as offered by manufacturers for their components will apply as well;
    b. The contractor must respond to non-critical system failure service calls within 24 hours of notification. For maintenance purposes, a non-critical system failure refers to any system deficiency requiring maintenance;
    c. For critical system failure service calls, response must be provided within four (4) hours of notification. For maintenance purposes, a critical system failure refers to a system failure that would prevent central monitoring of the facility.
24. Standard warranty as offered by the manufacturer of components does not replace the warranty of the Contractor's liability.