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
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

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 or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet Access Control System	
Solicitation No. - N° de l'invitation 0D160-204228/A	**Date** 2020-06-16
Client Reference No. - N° de référence du client 0D160-204228	
GETS Reference No. - N° de référence de SEAG PW-$$HN-329-78815	
File No. - N° de dossier hn329.0D160-204228	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-07-28**	**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: Dumaresq, Steve	**Buyer Id - Id de l'acheteur** hn329
Telephone No. - N° de téléphone (613) 296-1704 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

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
Electrical & Electronics Products Division
L'Esplanade Laurier
East Tower, 4th floor,
Ottawa
Ontario
K1A 0S5

Canada

SUBMISSION OF BIDS

In light of the current COVID-19 pandemic, it is recommended that all suppliers submit their bid using the epost Connect:
Given that many people are currently working from home and in an effort to reduce the spread of the Coronavirus disease (COVID-19) within communities, bidders are highly encouraged to transmit their bid electronically using the epost Connect service.

Bids must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

Note: For bidders choosing to submit using epost Connect for bids closing at the Bid Receiving Unit in the National Capital Region (NCR) the email address is:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

- - -

If you experience difficulties with the epost connect system, you may contact our Bids Receiving Unit at the following address for assistance:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Do not send any bid or offer directly to that address.

SITE VISITS NOT AVAILABLE

In light of the COVID-19 situation, Government restrictions on public gatherings and physical distancing requirements are limiting the ability to provide traditional site visits. Due to its immediate requirement, Public Safety Canada has decided to distribute detailed information about its current systems to interested bidders following the signature of a non-disclosure agreement. A teleconference will take place, in replacement of site visits, where all questions will be answered.

SPECIFICATIONS AVAILABLE ON USB KEY

Interested bidders must email the Contracting Authority to request a copy of the specifications that have been made available.

Bidder must include a completed Annex G, Non-disclosure Agreement for Solicitation and Contract, with the request for specifications for each individual that will have access to them.

Steve Dumaresq
Public Works and Government Services Canada - Acquisitions Branch
Logistics, Electrical, Fuel and Transportation Directorate - "HN" Division

steve.dumaresq@pwgsc-tpsgc.gc.ca

Note: The USB key will be sent by messenger service. Provide complete address and contact details.

BIDDERS' CONFERENCE (TELECONFERENCE)

Date, Time and Call-in Details of the bidders’ conference (teleconference) will be provided upon acceptance of bidder’s request for specifications USB Key.

The scope of the requirement outlined in the bid solicitation will be reviewed during the conference and questions will be answered. It is recommended that bidders who intend to submit a bid attend.

Bidders should provide, in writing, to the Contracting Authority, the name(s) of the person(s) who will be attending.

Any clarifications or changes to the bid solicitation resulting from the bidders' conference will be included as an amendment to the bid solicitation. Bidders who do not attend will not be precluded from submitting a bid.

PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications: includes the certifications to be provided;

Part 6 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Requirement, the Basis of Payment, Security Requirements, the Federal Contractors Program for Employment Equity - Certification, the Insurance Requirements and any other annexes.

1.2 Summary

1.2.1 Public Safety Canada (PS) has a requirement to upgrade their legacy Access Control/Intrusion System.

Initial requirement is for two (2) locations in Ottawa, Ontario: 269 Laurier and 340 Laurier.
Contract will include the option for future system upgrades and installations at various locations across Canada.

The work includes the design, supply, installation, testing and provision of operational and technical training on the Enterprise Integrated Security System Upgrade (EISS) as described in the Statement of Requirement. Refer to Annex A.

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Resulting Contract Clauses.

1.2.3 The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) and the Canadian Free Trade Agreement (CFTA).

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual* (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2020-05-28) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 120 days

2.2 Submission of Bids

In light of the current COVID-19 pandemic, it is recommended that all suppliers submit their bid using the epost Connect:
Given that many people are currently working from home and in an effort to reduce the spread of the Coronavirus disease (COVID-19) within communities, bidders are highly encouraged to transmit their bid electronically using the epost Connect service.

Bids must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

Note: For bidders choosing to submit using epost Connect for bids closing at the Bid Receiving Unit in the National Capital Region (NCR) the email address is:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than ten (10) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical 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 question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario. Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.5 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least fourteen (14) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

- If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the 2003 standard instructions. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.

  The bid must be gathered per section and separated as follows:

  Section I: Technical Bid
  Section II: Financial Bid
  Section III: Certifications
  Section IV: Additional Information

- If the Bidder chooses to submit its bid in hard copies, Canada requests that the Bidder submits its bid in separately bound sections as follows:

  Section I: Technical Bid (2 hard copies) and 2 soft copies on USB keys;
  Section II: Financial Bid (1 hard copy) and 1 soft copy on USB key;
  Section III: Certifications (1 hard copy) and 1 soft copy on USB key;
  Section IV: Additional Information (1 hard copy) and 1 soft copy on USB key.

  If there is a discrepancy between the wording of the soft copy on electronic media and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

- If the Bidder is simultaneously providing copies of its bid using multiple acceptable delivery methods, and if there is a discrepancy between the wording of any of these copies and the electronic copy provided through epost Connect service, the wording of the electronic copy provided through epost Connect service will have priority over the wording of the other copies.

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

(a) use 8.5 x 11 inch (216 mm x 279 mm) paper;
(b) use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Bidders should:

1) use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and

2) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Section II: Financial Bid

Bidders must submit their financial bid in accordance with all pricing requirements presented herein.

3.1.1 Exchange Rate Fluctuation Risk Mitigation

1. The Bidder may request Canada to assume the risks and benefits of exchange rate fluctuations. If the Bidder claims for an exchange rate adjustment, this request must be clearly indicated in the bid at time of bidding. The Bidder must submit form PWGSC-TPSGC 450, Claim for Exchange Rate Adjustments with its bid, indicating the Foreign Currency Component (FCC) in Canadian dollars for each line item for which an exchange rate adjustment is required.
2. The FCC is defined as the portion of the price or rate that will be directly affected by exchange rate fluctuations. The FCC should include all related taxes, duties and other costs paid by the Bidder and which are to be included in the adjustment amount.
3. The total price paid by Canada on each invoice will be adjusted at the time of payment, based on the FCC and the exchange rate fluctuation provision in the contract. The exchange rate adjustment will only be applied where the exchange rate fluctuation is greater than 2% (increase or decrease).
4. At time of bidding, the Bidder must complete columns (1) to (4) on form PWGSC-TPSGC 450, for each line item where they want to invoke the exchange rate fluctuation provision. Where bids are evaluated in Canadian dollars, the dollar values provided in column (3) should also be in Canadian dollars, so that the adjustment amount is in the same currency as the payment.
5. Alternate rates or calculations proposed by the Bidder will not be accepted for the purposes of this exchange rate fluctuation provision.

Section III: Certifications

Bidders must submit the certifications required under Part 5.

Compliance with the certifications provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the term of the Contract. If the Contractor does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

Section IV: Additional Information

3.1.2 Contractor's Representative

Name and telephone number of the person responsible for:

General enquiries		**Delivery follow-up**	
Name:	_____	Name:	_____
Telephone:	_____	Telephone:	_____
Facsimile:	_____	Facsimile:	_____
E-mail:	_____	Facsimile:	_____

3.1.3 Warranty Repairs

It may be necessary for warranty repairs to be performed on site. You are requested to provide response time and location of nearest office/depot providing staff for this work. The contact person is as follows:

Response Time: _____
Name: _____
Telephone No.: _____
Facsimile No.: _____
Email/Internet Address: _____

3.1.4 Emergency Services/Repairs

If requested by the technical authority, the Contractor shall be required to provide on-site emergency service/repairs not covered under the warranty provision of the General Conditions 2030 during the contract period. The contact person is as follows:

Name: _____
Telephone No.: _____
Facsimile No.: _____
Email/Internet Address: _____

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

For the purpose of the Evaluation Process only, **"Bidder"** means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It may also include the parent or subsidiaries of the Bidder.

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical, management, support and financial evaluation criteria.

(b) An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

The Technical, Management and Support Bids should be concise and address, but not necessarily be limited to, the points that are subject to the evaluation criteria against which the Bid will be evaluated.

Bidders should address the evaluation criteria in sufficient depth in their bid. Simply repeating the statement contained in the solicitation document is not sufficient. Bidders should explain and demonstrate how they propose to meet the requirements and how they will carry out the Work.

The bidder is reminded to provide as much technical information and documentation as possible, so as to fully demonstrate technical compliance to all elements of the solicitation, otherwise proposal may be deemed non-compliant (non-responsive) for insufficient information.

4.1.1.1 Mandatory Technical Criteria

Simply stating a compliancy to a criteria is insufficient. Bidders must present a clearly organized, printed (i.e., not handwritten) proposal that includes all necessary technical and descriptive information, in order to clearly demonstrate their compliancy to all items presented in the Statement of Requirement (STR) at Annex A, as well as related specifications.

Two (2) initial sites: 269 Laurier (Ottawa) and 340 Laurier (Ottawa)

For each site:
a) Compliance to all requirements presented in this solicitation;
b) Technical compliance to the Statement of Requirement at Annex A;
c) Technical compliance to the mandatory evaluation criteria presented at Annex B;
d) Bidder must submit a complete security solution for each site with all necessary technical information and documentation to demonstrate compliance to the requirement presented herein.

Responses will be evaluated on a simple, stringent pass/fail basis. Proposals not meeting each mandatory requirement will be considered non-responsive (non-compliant) and given no further consideration.

4.1.1.2 Point Rated Technical Criteria

a) Compliance to the point rated evaluation criteria presented at annex B;
b) 5 points will be awarded for each additional year of project experience of similar size and scope (after 5 years of mandatory experience identified at M1). (Max. of 15 points).

4.1.2 Financial Evaluation

a) Compliance with the pricing requirements presented herein;
b) Compliance and completion of an Annex C, Pricing Schedule.

4.1.2.1 Pricing Basis

Firm prices in Canadian dollars, DDP Delivered Duty Paid (destination), with all applicable Custom duties and Excise taxes included. Freight charges to destination included. Goods and Services Tax (GST) and/or the Harmonized Sales Tax (HST) not included.

If Bidder is requesting the exchange rate fluctuation protection, a completed Claim for Exchange Rate Adjustments form (PWGSC-TPSGC 450) must be included with submitted bid.

4.1.3 Basis of Selection - Lowest Price Per Point

To be declared responsive, a bid must:

a) comply with all the requirements of the bid solicitation; and
b) meet all mandatory technical evaluation criteria.

Bids not meeting (a) or (b) will be declared non-responsive. Neither the responsive bid that receives the highest number of points nor the one that proposed the lowest price will necessarily be accepted.

The responsive bid with the lowest price per point will be recommended for award of a contract.
Lowest Price Per Point = Total Evaluated Bid $ (site 1+ site 2) / Number of Rated Points obtained (max. 15).

PART 5 – CERTIFICATIONS

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Declaration of Convicted Offences

If applicable, pursuant to subsection Declaration of Convicted Offences of section 01 of the Standard Instructions, the Bidder must provide with its bid, a completed Declaration Form (http://www.tpsgc-pwgsc.gc.ca/ci-if/formulaire-form-eng.html), to be given further consideration in the procurement process.

5.1.2 Status and Availability of Resources

The Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in its bid, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, retirement, resignation, dismissal for cause or termination of an agreement for default.

If the Bidder has proposed any individual who is not an employee of the Bidder, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

_____ _____

Signature ***Date***

5.1.3 Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

_____ _____

Signature ***Date***

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.1 Integrity Provisions – List of Names

Bidders who are incorporated, including those bidding as a joint venture, must provide a complete list of names of all individuals who are currently directors of the Bidder.

Bidders bidding as sole proprietorship, as well as those bidding as a joint venture, must provide the name of the owner(s).

Bidders bidding as societies, firms or partnerships do not need to provide lists of names.

5.2.2 Federal Contractors Program for Employment Equity - Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list (http://www.labour.gc.ca/eng/standards_equity/eq/emp/fcp/list/inelig.shtml) available from Employment and Social Development Canada (ESDC) - Labour's website.

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid " list at the time of contract award.

5.2.3 General Environmental Criteria Certification

The Bidder must select and complete one of the following two certification statements.

A) The Bidder certifies that the Bidder is registered or meets ISO 14001.

_____ _____

Bidders' Authorized Representative Signature **Date**

OR

B) The Bidder certifies that the Bidder meets and will continue to meet throughout the duration of the contract, a minimum of four (4) out of six (6) criteria identified in the table below.

The Bidder must indicate which four (4) criteria, as a minimum, are met.

Green Practices within the Bidders' organization	**Insert a checkmark for each criterion that is met**
Promotes a paperless environment through directives, procedures and/or programs	
All documents are printed double sided and in black and white for day to day business activity unless otherwise specified by your client	
Paper used for day to day business activity has a minimum of 30% recycled content and has a sustainable forestry management certification	
Utilizes environmentally preferable inks and purchase remanufactured ink cartridges or ink cartridges that can be returned to the manufacturer for reuse and recycling for day to day business activity.	
Recycling bins for paper, newsprint, plastic and aluminum containers available and emptied regularly in accordance with local recycling program.	
A minimum of 50% of office equipment has an energy efficient certification.	

_____ _____

Bidders' Authorized Representative Signature **Date**

PART 6 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

1. Security Requirement

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of **Protected**, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC);
2. This contract includes access to Controlled Goods. Prior to access, the contractor must be registered in the Controlled Goods Program (CGP) of PWGSC;
3. The Contractor/Offeror personnel requiring access to protected information, assets or work site(s) must EACH hold a valid **Reliability Status**, granted or approved by the CISD/PWGSC;
4. The Contractor must not utilize its Information Technology systems to electronically process, produce or store protected information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed up to the level of **Protected;**
5. Subcontracts which contain security requirements are not to be awarded without the prior written permission of CISD/PWGSC;
6. The Contractor/Offeror must comply with the provisions of the:
    1. Security Requirements Check List and security guide (if applicable), attached at Annex;
    2. Industrial Security Manual (Latest Edition).

2. Statement of Requirement

The Contractor shall design, supply, install, test and provide security solutions in accordance with the Statement of Requirement, related material and technical requirements presented herein.

2.1 Initial requirement

Two (2) sites: 269 Laurier (Ottawa) and 340 Laurier (Ottawa)

2.2 Optional requirement – Future expansion

The exact nature and scope of the work for requirements in regional offices will be determined at a later time when the requirement and location is known. Other sites may include, but are not limited to: Burnaby (BC), Edmonton (AB), Regina (SK), Winnipeg (MB), Fredericton (NB), Toronto (ON), Ottawa (ON), Montreal (QC), Dartmouth (NS), Charlottetown (PEI), St. John’s (NL).

3. Task Authorizations

The Work or a portion of the Work to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract.

3.1 Task Authorization Process

1. The Technical Authority will provide the Contractor with a description of the task using the Task Authorization form specified as annex to the contract.
2. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis (bases) and methods of payment as specified in the Contract.

3. The Contractor must provide the Technical Authority, within 5 calendar days of its receipt, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract.
4. The Contractor must not commence work until a TA authorized by the Technical Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

3.2 Individual Task Authorization Limit

All task authorizations must be authorized by the Contracting Authority before issuance.

3.3 Periodic Usage Reports - Contracts with Task Authorizations

The Contractor must compile and maintain records on its provision of services to the federal government under authorized Task Authorizations issued under the Contract.

The Contractor must provide this data in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "nil" report.

The data must be submitted on a quarterly basis *to* the Contracting Authority.

The quarterly periods are defined as follows:
1st quarter: April 1 to June 30;
2nd quarter: July 1 to September 30;
3rd quarter: October 1 to December 31; and
4th quarter: January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 30 calendar days after the end of the reporting period.

Reporting Requirement- Details:
A detailed and current record of all authorized tasks must be kept for each contract with a task authorization process. This record must contain:

For each authorized task:
i. the authorized task number or task revision number(s);
ii. a title or a brief description of each authorized task;
iii. the total estimated cost specified in the authorized Task Authorization (TA) of each task, exclusive of Applicable Taxes;
iv. the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;
v. the start and completion date for each authorized task; and
vi. the active status of each authorized task, as applicable.

For all authorized tasks:
i. the amount (exclusive of Applicable Taxes) specified in the contract (as last amended, as applicable) as Canada's total liability to the contractor for all authorized TAs; and
ii. the total amount, exclusive of Applicable Taxes, expended to date against all authorized TAs.

4. Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

4.1 General Conditions

2030 (2020-05-28), General Conditions - Higher Complexity - Goods, apply to and form part of the Contract.

4.2 Supplemental General Conditions

4001 (2015-04-01) Hardware Purchase, lease and Maintenance;
4003 (2010-08-16) Licensed Software;
4004 (2013-04-25) Maintenance and Support Services for Licensed Software.

4.3 SACC Manual Clauses

B1501C (2018-06-21) Electrical Equipment
A9068C (2010-01-11) Site Regulations
A2000C (2006-06-16) Foreign Nationals (Canadian Contractor)
A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

5. Term of Contract

5.1 Initial Period of the Contract

The period of validity of this contract is for three (3) years, hence from __date__ to ___date___ inclusively.

5.2 Option(s) to Extend the Period of Contract

The Contractor grants to Canada the irrevocable option(s) to extend the term of the Contract by up to two (2) additional one (1) year period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Option Period One (1): From ___date___ to ___date___ inclusively;
Option Period Two (2): From ___date___ to ___date___ inclusively.

Canada may exercise this option at any time by sending a written notice to the Contractor before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

6. Authorities

6.1 Contracting Authority

Steve Dumaresq
Public Works and Government Services Canada - Acquisitions Branch
Logistics, Electrical, Fuel and Transportation Directorate - "HN" Division
L'Esplanade Laurier (LEL), 140 O'Connor Street, East Tower
Telephone: (613) 296-1704
E-mail address: steve.dumaresq@pwgsc-tpsgc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

6.2 Technical Authority

Name: ____
Telephone: ____
Facsimile: ____
E-mail: ____

The Technical Authority named above is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

6.3 Contractor's Representative

General enquiries		**Delivery follow-up**	
Name:	_____	Name:	_____
Telephone:	_____	Telephone:	_____
Facsimile:	_____	Facsimile:	_____
E-mail:	_____	Facsimile:	_____

6.4 Warranty Repairs

The contact person for warranty repairs to be performed on site as it may be necessary is as follows:

Response Time: _____
Name: _____
Telephone: _____
Facsimile: _____
E-mail: _____

6.5 Emergency Services/Repairs

If requested by the technical authority, the Contractor shall be required to provide on-site emergency service/repairs not covered under the warranty provision of the General Conditions 2030 during the contract period. The contact person is as follows:

Name: _____
Telephone: _____
Facsimile: _____
E-mail: _____

7. Payment

7.1 Basis of Payment

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm lot price for the equipment, installation and testing, travel expenses, on-site training, as-built drawings and manuals as specified in the Contract. Customs duties are included and Applicable Taxes are extra.

The Contractor will be paid firm hourly rates for work associated with emergency repairs, delays and performed in accordance with the Contract. Customs duties are included and Applicable Taxes are extra.

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work, unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

7.1.1 Task Authorizations

The Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the Work specified in the authorized Task Authorization (TA), as determined in accordance with the Basis of Payment in Annex B, to the limitation of expenditure specified in the authorized Task Authorization.

Canada's liability to the Contractor under the authorized Task Authorization must not exceed the limitation of expenditure specified in the authorized TA. Customs duties are included and Applicable Taxes are extra.

No increase in the liability of Canada or in the price of the Work specified in the authorized TA resulting from any design changes, modifications or interpretations of the Work will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been authorized, in writing, by the Contracting Authority before their incorporation into the Work.

7.1.2 Travel for Task Authorized Work

The Contractor will be reimbursed for the authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for overhead or profit, in accordance with the meal, private vehicle and incidental expense allowances specified in Appendices B, C and D of the *National Joint Council Travel Directive* and with the other provisions of the directive referring to "travellers", rather than those referring to "employees".

All travel must have the prior authorization of the Technical Authority. All payments are subject to government audit.

7.2 Limitation of Price

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

7.3 Limitation of Expenditure - Cumulative Total of all Task Authorizations

1. Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (TAs), inclusive of any revisions, must not exceed the sum of $ __ . Customs duties and Applicable Taxes are included.

2. No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

3. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

   a. when it is 75 percent committed, or

   b. four (4) months before the contract expiry date, or

   c. as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized TAs, inclusive of any revisions,
   whichever comes first.

4. If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority, a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

7.4 Discretionary Audit

The Contractor's certification that the price or rate is not in excess of the lowest price or rate charged anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both, is subject to verification by government audit, at the discretion of Canada, before or after payment is made to the Contractor.

If the audit demonstrates that the certification is in error after payment is made to the Contractor, the Contractor must, at the discretion of Canada, make repayment to Canada in the amount found to be in excess of the lowest price or rate or authorize the retention by Canada of that amount by way of deduction from any sum of money that may be due or payable to the Contractor pursuant to the Contract.

If the audit demonstrates that the certification is in error before payment is made, the Contractor agrees that any pending invoice will be adjusted by Canada in accordance with the results of the audit. It is further agreed that if the Contract is still in effect at the time of the verification, the price or rate will be lowered in accordance with the results of the audit

7.5 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

7.6 Monthly Payments

SACC Manual Clause H1008C (2008-05-12) Monthly Payments

7.7 Invoicing Instructions

1. The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions.

2. By submitting invoices the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.

7.8 Travel and Living Expenses

The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the *National Joint Council Travel Directive* and with the other provisions of the directive referring to "travellers", rather than those referring to "employees".

All travel must have the prior authorization of the Technical Authority.
All payments are subject to government audit.

8. Certifications - Compliance

The continuous compliance with the certifications provided by the Contractor in its bid and the ongoing cooperation in providing additional information are conditions of the Contract. Certifications are subject to verification by Canada during the entire period of the Contract. If the Contractor does not comply with any certification, fails to provide the additional information, or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

9. Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

10. Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

(a) the Articles of Agreement;
(b) the supplemental general conditions:
  (i) 4001 (2015-04-01) Hardware Purchase, lease and Maintenance;
  (ii) 4003 (2010-08-16) Licensed Software;
  (iii) 4004 (2013-04-25) Maintenance and Support Services for Licensed Software;
(c) the general conditions 2030 (2020-05-28), General Conditions - Higher Complexity - Goods;
(d) Annex __, Statement of Requirement;
(e) Annex __, Pricing and Basis of Payment;
(f) the signed Task Authorizations (including all of its annexes, if any);
(g) Annex __, Security Requirements Check List (SRCL);
(h) the Contractor's bid dated __.

11. Insurance

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

12. Disclosure of Information

The Contractor shall keep confidential and shall not publish or otherwise reuse, release, disclose or make available to any third party any Background or Foreground Information concerning as built drawings, site drawings and manuals, except as may be necessary to carry out the Work under the Contract in which case the Contractor shall impose the same obligation of confidentiality on any person to whom the information is disclosed.

ANNEX A STATEMENT OF REQUIREMENT (ATTACHED)
ANNEX B TECHNICAL EVALUATION CRITERIA (ATTACHED)

ANNEX C PRICING AND BASIS OF PAYMENT

PART 1 SECURITY SOLUTIONS FOR 269 LAURIER (OTTAWA) AND 340 LAURIER (OTTAWA)

SITE ONE: 269 LAURIER (OTTAWA)

Firm prices in Canadian dollars, DDP Delivered Duty Paid (destination), with all applicable Custom duties and Excise taxes included. Freight charges to destination included. All costs related to travel and living expenses included. Goods and Services Tax (GST) and/or the Harmonized Sales Tax (HST) not included.

If Bidder is requesting the exchange rate fluctuation protection, a completed Claim for Exchange Rate Adjustments form (PWGSC-TPSGC 450) must be included with submitted bid.

Lot Price Cost Breakdown
Prior to contract award, the successful bidder must provide a line by line breakdown of all prices provided within Annex C – Pricing and Basis of Payment. The pricing provided will be used to calculate the cost of any Task Authorizations throughout the life of the contract.

CONTRACTOR PROPOSED SOLUTION for 269 Laurier (Ottawa)

1. DESIGN OF THE SYSTEM

Firm Lot Price for the design

DESIGN	***LOT PRICE: $_____***

2. DELIVERY OF EQUIPMENT

Firm Lot Price for all related equipment, excluding spare parts.

EQUIPMENT	***LOT PRICE: $_____***

3. INSTALLATION

INSTALLATION	***LOT PRICE: $_____***

4. SOFTWARE INTEGRATION AND TESTING

SOFTWARE INTEGRATION	***LOT PRICE: $_____***
TESTING COST	***LOT PRICE: $_____***

5. ON-SITE TRAINING AND DOCUMENTATION

ON-SITE TRAINING COST	***LOT PRICE: $_____***

AS-BUILT DRAWINGS AND SCHEMATICS	***LOT PRICE: $_____***

MANUALS	***LOT PRICE: $_____***

6. SERVICE AGREEMENT FOR SUPPORT AND MAINTENANCE

SERVICE AGREEMENT	**Price – 1 year**
In accordance with Annex A	$

SUPPLIER PROPOSED SOLUTION for 269 Laurier (Ottawa)	***TOTAL BID PRICE: $_____*** ***Sum of line items 1 to 6 above***

ANNEX C – PRICING AND BASIS OF PAYMENT (continued)

SITE TWO: 340 LAURIER (OTTAWA)

Firm prices in Canadian dollars, DDP Delivered Duty Paid (destination), with all applicable Custom duties and Excise taxes included. Freight charges to destination included. All costs related to travel and living expenses included. Goods and Services Tax (GST) and/or the Harmonized Sales Tax (HST) not included.

If Bidder is requesting the exchange rate fluctuation protection, a completed Claim for Exchange Rate Adjustments form (PWGSC-TPSGC 450) must be included with submitted bid.

Lot Price Cost Breakdown
Prior to contract award, the successful bidder must provide a line by line breakdown of all lot prices provided within Annex C – Pricing and Basis of Payment. The pricing provided will be used to calculate the cost of any Task Authorizations throughout the life of the contract.

CONTRACTOR PROPOSED SOLUTION for 340 Laurier (Ottawa)

1. DESIGN OF THE SYSTEM

Firm Lot Price for the design

DESIGN	***LOT PRICE: $_____***

2. DELIVERY OF EQUIPMENT

Firm Lot Price for all related equipment, excluding spare parts.

EQUIPMENT	***LOT PRICE: $_____***

3. INSTALLATION

INSTALLATION	***LOT PRICE: $_____***

4. SOFTWARE INTEGRATION AND TESTING

SOFTWARE INTEGRATION	***LOT PRICE: $_____***
TESTING COST	***LOT PRICE: $_____***

5. ON-SITE TRAINING AND DOCUMENTATION

ON-SITE TRAINING COST	***LOT PRICE: $_____***

AS-BUILT DRAWINGS AND SCHEMATICS	***LOT PRICE: $_____***

MANUALS	***LOT PRICE: $_____***

6. SERVICE AGREEMENT FOR SUPPORT AND MAINTENANCE

SERVICE AGREEMENT	**Price – 1 year**
In accordance with Annex A	$

SUPPLIER PROPOSED SOLUTION for 340 Laurier (Ottawa)	***TOTAL BID PRICE: $_____*** ***Sum of items 1 to 6 above***

TOTAL EVALUATED BID:

SITE 1

SUPPLIER PROPOSED SOLUTION for 269 Laurier (Ottawa)	***TOTAL BID PRICE: $_____***

PLUS

SITE 2

SUPPLIER PROPOSED SOLUTION for 340 Laurier (Ottawa)	***TOTAL BID PRICE: $_____***

TOTAL EVALUATED BID (Site 1 + Site 2)	***TOTAL BID PRICE: $_____***

ANNEX C – PRICING AND BASIS OF PAYMENT (continued)

PART 2 OPTION - FUTURE EXPANSIONS
Pricing will be used for individual Task Authorizations

1. MSRP PRICE DISCOUNTS ON EQUIPMENT AND SPARES

The bidder must provide a list of manufacturers (OEM) represented and must quote one (1) firm percentage discount off Manufacturer Suggested Retail Price list (MSRP) for each OEM listed. Discount will be based on US$ pricing only if CDN$ pricing is not available.

Manufacturer (OEM)	Firm percentage discount off MSRP	Discount percentage based on US$ or CDN$
	%	
	%	
	%	
	%	
	%	
	%	

2. INSTALLATION (FIRM HOURLY RATES)

The bidder must submit a firm hourly rate for installation during and outside normal working hours for each labour category required.

Normal working hours are Monday to Friday, 7:00 AM to 17:00 PM with exception of statutory holidays.

Labour Categories	Hourly Rate During Regular Hours	Hourly Rate Outside Regular Hours
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

3. SOFTWARE INTEGRATION (FIRM HOURLY RATES)

The bidder must submit a firm hourly rate for software integration during and outside normal working hours for each labour category required.

Labour Categories	Hourly Rate During Regular Hours	Hourly Rate Outside Regular Hours
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

4. TESTING OF EQUIPMENT (FIRM HOURLY RATES)

The bidder must submit a firm hourly rate for testing of equipment during and outside normal working hours for each labour category required.

Labour Categories	Hourly Rate During Regular Hours	Hourly Rate Outside Regular Hours
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

ANNEX D to PART 5 - CERTIFICATIONS

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act*.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

ANNEX E TASK AUTHORIZATION FORM PWGSC-TPSGC 572

See: http://publiservice-app.pwgsc.gc.ca/forms/pdf/572.pdf

ANNEX F SECURITY REQUIREMENTS CHECK LIST (SRCL)

(attached)

ANNEX G NON-DISCLOSURE AGREEMENT – SOLICITATION AND CONTRACT

(attached)

ANNEX H FORM PWGSC-TPSGC 450, CLAIM FOR EXCHANGE RATE ADJUSTMENTS

(attached)

Annex “A”

Statement of Requirements

Public Safety Canada – Sécurité publique Canada (PS/SP)

Public Safety / Sécurité publique –
Enterprise Integrated Security System (PSSP-EISS)

TABLE OF CONTENTS

TITLE

Public Safety / Sécurité publique – Enterprise Integrated Security System Upgrade (PSSP-EISS)

OBJECTIVE

Public Safety / Sécurité publique Canada (PSSP) National Headquarters in the National Capital Region currently has a requirement to upgrade their legacy Access Control/Intrusion System. The current legacy systems are based on 1. Summit Enterprise eNT and 2. ICT Protégé System. The requirement is to upgrade to a centralized modern Enterprise Integrated Security System with which to protect, defend and respond to actual and potential security and life-safety events and situations affecting its people, assets and information.

PS/SP currently operates using Summit eNT on multiple floors in the National Capital Region at 269 Laurier. A second building 340 Laurier currently has an independent ICT ACS system. Both buildings use a common proximity card with the same format.

The objective of this contract is to have both buildings with the possibility of future others, operate under one single centralized integrated system.

In light of the COVID-19 situation, Government restrictions on public gatherings and physical distancing requirements are limiting the ability to provide traditional site visits. Due to its immediate requirement, Public Safety Canada has decided to distribute detailed information about its current systems to interested bidders following the signature of a non-disclosure agreement. A teleconference will take place, in replacement of site visits, where all questions will be answered.

PS/SP operates in numerous Regional Offices across Canada and the long-term vision is to have those locations integrated on to the new system platform. Therefore, the proposed system must be expandable for future regional offices integration and be monitored and managed from 269 Laurier W. in Ottawa, ON.

PS/SP requires a maintenance and servicing contract with the successful Bidder upon completion of the upgrade (Section – S).

INTRODUCTION

The purpose of this document is to describe the Statement of Requirements for PSSP-EISS. This document represents a consolidation of the technical and functional requirements for the PSSP-EISS. The requirements identify the PSSP-EISS infrastructure, features and functionality needed to support the Department of Public Safety / sécurité publique Canada and all its facilities in Canada.

Physical security is the means by which PS/SP implements measures to safeguard employees, assets and information. The foundations for the development of this Statement of Requirements are the RCMP Guidelines related to protection, detection and response. While PSSP has established a series of standards for the definition, design and implementation of physical security strategies, these guidelines provide a well-researched methodology for enhanced architectural, technology and personnel solutions. Citing from G1-025:

> **Protection** is achieved through the use of physical, procedural and psychological barriers to delay or deter unauthorized access. Protective barriers should: deter an attacker, mark the perimeter of a restricted area, delay or prevent access, protect a person or asset from a threat, contain a person or asset from a threat or impede escape.
>
> **Detection** involves the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred. There are four steps to detection: notice of the event, convey information regarding the event to an analysis center, analyze the information received and evaluate it and if it is deemed that the event is unauthorized, then initiate intervention.
>
> In the context of physical security, **Response** entails the implementation of measures to ensure that security incidents are reported to appropriate security officials and immediate and long-term corrective action is taken in a timely fashion. Effective response strategies should be based on: the adversaries and their qualities, the ability of the responders to reach the asset or the target and capabilities of the responders.

The technical aspects of these key elements of a sound physical security strategy are described within the contents of this Statement of Requirements

BACKGROUND

Public Safety / Sécurité publique Canada (PS/SP) is Canada's lead department with the mandate to keep Canadians safe from a range of risks such as natural disasters, crime and terrorism. Public Safety Canada works with other federal departments, other levels of government, first responders, community groups, the private sector and other countries to achieve its objectives. The Department plays a key role in developing policies, delivering programs and ensuring cohesion and integration on policy and program issues within the Public Safety Portfolio, which includes: national security, emergency management, law enforcement, border management, corrections, and crime prevention.

PS/SP is embarking on a project to upgrade, renew and enhance its aging Access Control and Intrusion Alarm Systems, which have been deployed in the National Capital Region (NCR). The scope of this document is to define the technical and functional business requirements for the PSSP-EISS. This functionality is required to support the business objectives of the stakeholders in order to fulfill their respective mandates. The following illustrates the functionality and capabilities of the PSSP-EISS, as required by the stakeholders.

- Electronic Access Control
- Intrusion Alarm System Management & Integration
- Network Infrastructure and Security
- Maintenance, Service Calls, and Response.
- Security Operations

CONCEPT OF OPERATIONS

The PSSP-EISS includes security software, hardware and equipment designed, procured and installed to ensure the safety, security and protection of people, property and assets. The PSSP-EISS must provide its users with the tools and applications required to manage people, property, and monitor the activities at the site. The system is based on a centralized HQ infrastructure that is flexible and configurable to allow the proper management of different processes and procedures in order to achieve the security goals of PS/SP. All hardware and software purchased must remain the property of PS/SP and therefore the PS/SP qualified staff of the security department are to have unobstructed access to all aspects and components of the proposed system during and after the installation.

SECTION A – PSSP-EISS APPLICATIONS

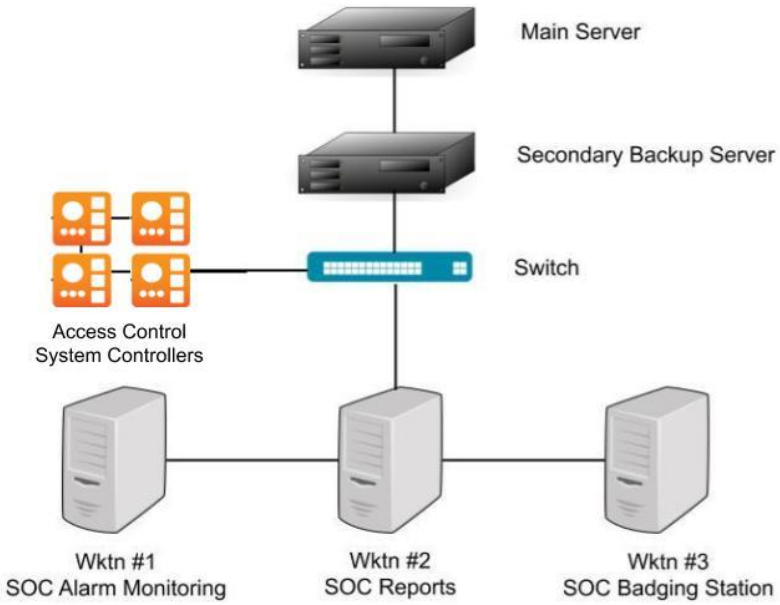
The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must provide the following enterprise-class integrated physical security applications:

a. Electronic Access Control
b. Personnel Identification Management
c. Intrusion Detection, Monitoring, Control and Reporting
d. Input/output Control and Management
e. Digital Video Surveillance and Management Integration Capable
f. Visitor Management
g. Elevator Control
h. Duress System Integration
i. Management Reporting & Auditing

SECTION B – PUBLIC SAFETY/SÉCURITÉ PUBLIQUE – ENTRPRISE INTEGRATED SECURITY SYSTEM (PSSP-EISS) ARCHITECTURE

1. The PSSP-EISS must be configured such that a Primary Master Server must be located at 269 Laurier Headquarters (HQ) in Ottawa, Ontario, Canada on which the Security Application Software and its associated data/database must reside. The Primary Master Server must be accompanied by a Secondary Master Server (located at 340 Laurier W.) which must be installed in a fully redundant configuration to provide operational reliability and data integrity. Existing CCTV Recorders both located at the HQ as well as both remote sites are not apart of this project to be integrated, however the new proposed access control system is required to be integrated with a video system to display video on alarm trigger for future requirements.

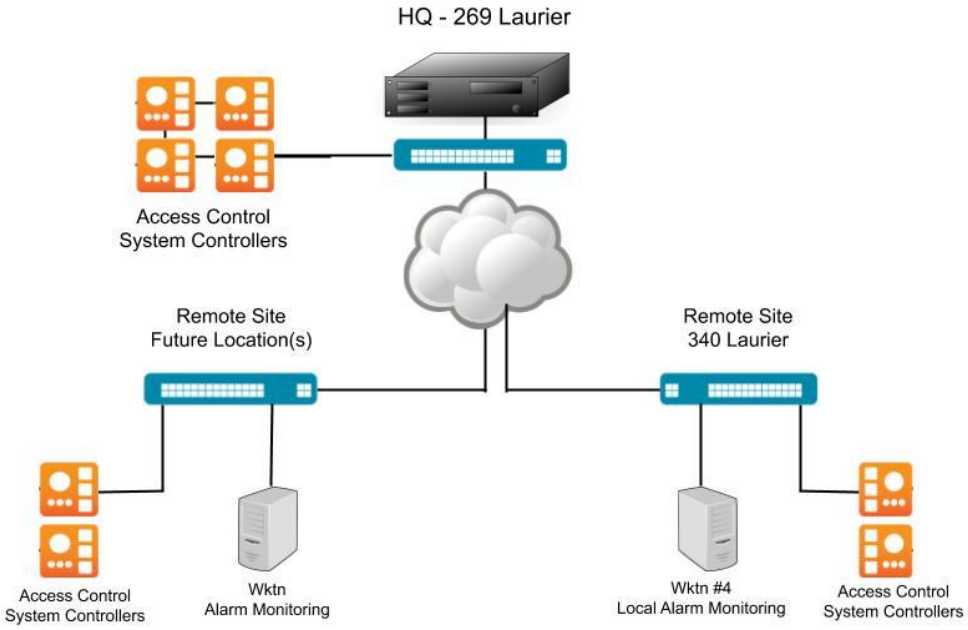
Figure 1 - Core System Architecture HQ
Security Operations Center



It must be the vendor's responsibility to provide all security application software, licenses, equipment hardware, network cabling for controllers, and any other peripherals that may be required to support the installation. Network Servers, workstations and switches are not to be supplied by the vendor they must be procured internally however the vendor must be responsible to communicate with PS/SP the application & hardware requirements for:

- Server(s)
- Workstations

Figure 2 - Network System Architecture HQ Locations Outside of Headquarters



SECTION C – PSSP-EISS CORE SYSTEM

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must be based on a client server architecture and reside on the PS network infrastructure. The PSSP-EISS must allow the distribution of functions such as video surveillance, access control alarm monitoring and control, credential management and photo identification processing across the network such that these functions are available from any PSSP-EISS Server or PSSP-EISS Workstation on the network. The PSSP-EISS must be integrated into one operating environment and must use an integrated relational database for all functionality.

2. The PSSP-EISS must be provided in a fully redundant architecture for each of the Primary and Secondary Servers. The PSSP-EISS must support high availability, fault tolerant hardware, software, storage and product solutions and architecture and deliver a fully redundant database and operational hot standby capability. The PSSP-EISS redundant configuration must allow for normal operations to occur in the event of a server failure at which time the switchover to the backup (or secondary) server from the primary server must be automatic and not impede or degrade the operation of the PSSP-EISS.

3. The PSSP-EISS must be configured such that the following servers and workstations form the core of the system:
    i. PSSP-EISS Master Server 1 (Primary) (HQ)
    ii. PSSP-EISS Master Server 2 (Secondary) (340 Laurier W.)
    iii. PSSP-EISS Administrator / Operator Workstation SOC (HQ)
    iv. PSSP-EISS Alarm Monitoring Workstation SOC (HQ)
    v. PSSP-EISS Identification Management Workstation (HQ)
    vi. PSSP-EISS Alarm Monitoring Workstation (Remote Site)

4. The PSSP-EISS Primary Master Server must reside at HQ in Ottawa, Ontario, Canada and must contain all the operating and administrative data and functionality for the entire PSSP-EISS. The Secondary Master Server must be in located in another building (340 Laurier W.). The PSSP-EISS must support the future configuration of disaster recovery (DR) in an offsite location in the event both Master and Secondary servers are not reachable. Describe how the proposed PSSP-EISS supports this requirement.

5. The PSSP-EISS Administrator / Operator Workstation must provide a facility for the configuration, management and reporting of all system programming, credential functions, alarm and event programming and hardware operating parameters. It may also serve as a training workstation for new Security Operations Centre guards. User rights must govern access (read/write) privileges to the applications, modules, data and records in the PSSP-EISS.

6. The PSSP-EISS Alarm Monitoring Workstation must provide a facility for the monitoring and reporting of the access control system alarms and events. User rights must govern access (read/write) privileges to the applications, modules, data and records in the PSSP-EISS.

7. The PSSP-EISS Identification Management Workstation (Remote Site) must provide a facility for the enrollment of credential holders, the capture of photographs, signature and data from the credential holder and the generation of physical credentials (e.g., photo identification badges). User rights must govern access (read/write) privileges to the applications, modules, data and records in the PSSP-EISS. *Identification Management and Badge Printing and Design must be compatible with existing equipment.

8. The PSSP-EISS Alarm Monitoring Workstation (Remote Site) must provide an offsite facility for local monitoring and reporting of the access control system alarms and events. User rights must govern access (read/write) privileges to the applications, modules, data and records in the PSSP-EISS.

9. The system must be made up of the following major components:
    i. Master PSSP-EISS Server (Primary), Master PSSP-EISS Server (Secondary), PSSP-EISS Administrator Workstation, PSSP-EISS Alarm Monitoring Workstations and PSSP-EISS Identification Management Workstation
    ii. Secure Network
    iii. Network Devices and Components
    iv. Security Panels
    v. Security Devices and Components (e.g. credential readers, locking devices, alarm sensors)

10. Each of these major components must be integrated to operate as a fully functional, complete turnkey systems solution.

11. It is Mandatory for the proposed PSSP-EISS to encompass and utilize the already installed access control devices at each door. Such devices include:

    i. Card Readers – (to be replaced with new)
    ii. Request to Exit Devices – Kantech T-Rex
    iii. Door Contacts - Various
    iv. Electric Strikes – 12VDC/24VDC - Various
    v. Electrified Levers – 24V - Various
    vi. Sirens/Piezos – 12-24VDC - Various

12. Any PSSP-EISS workstation on the network must be capable of performing data entry, alarm handling and processing, and system management functions.

13. The PSSP-EISS must be flexible and scalable in architecture, permitting expansion of both capacity and functionality; to be implemented progressively as needed, through software licensing and/or software upgrades while maintaining network operations.

14. The PSSP-EISS must allow, but not require, separation of the database server, file server, application server and web server roles to support multi-tier server architecture.

15. It is required that the PSSP-EISS system be capable of supporting database and file replication similar to Microsoft SQL Server Replication Services and Microsoft Distributed File System Replication (DFSR) for providing distributed database replication across the PSSP-EISS application servers, allowing for system expansion and delivering tiers of server redundancy. Describe how the proposed PSSP-EISS supports this requirement.

16. The PSSP-EISS system must be designed using an IP-centric architecture and must conform to the standard TCP/IP networking communications protocols between its components, including routing and firewall traversal capabilities.

17. It is required that the PSSP-EISS supports a nested or layered zoning strategy such that public, reception, operation, security and high security zones can be managed independently and interactively. It is required that such zones be defined in the PSSP-EISS and include various access devices (e.g., readers, keypads) or intrusion devices (e.g., motion detectors, door contacts, local alarm control keypads). It is required that once a zone is defined, the PSSP-EISS provide a facility for programming the posture and operation of each zone independently. Examples of such postures include: mask entire zone, unmask entire zone, or define anti-pass back rules between zones. Describe how the proposed PSSP-EISS supports these requirements.

18. For the term of the contract, the vendor must ensure that all security panels and associated modules are backwards compatible. The vendor must also ensure that all security panels and associated hardware provided during the term of the contract are supported by the most up to date software and firmware releases, versions, updates, upgrades and maintenance releases. The vendor must also ensure that all power supplies, batteries, and power converters are adequate to support the installations.

SECTION D – PLATFORM AND INFRASTRUCTURE REQUIREMENTS

As the PSSP-EISS relies on our internal network infrastructure to transport, process and store its access, alarm video and other information and data, it is critical that the PSSP-EISS meet PSSP's IT/IM standards, policies, programs and equipment. The following section outlines the requirements associated with the department's computing platform standards, databases, networking architecture and strategies, IT security policies, operating system and application-specific environments and other technical items which must be met by the new PSSP-EISS.

Platform and Operating Environment

1. The PSSP-EISS must operate on a server hardware platform that is adequate for the proposed system's requirement and that offers all the processing, memory, storage and networking capabilities to operate the system reliably. The servers must be housed in an operational security operations centre environment by others.

2. The PSSP-EISS must operate on a workstation hardware platform that is adequate for the proposed system's requirements with enough processing, memory, storage and networking capabilities to operate reliably. The workstations must be housed in secure operation zones by others.

3. The PSSP-EISS hardware must communicate over the currently legacy topology and the vendor must ensure supplied hardware communicating over the network has the ability of security encryption through proper configurations.

4. The PSSP-EISS application must not require separate physical devices (e.g. hardware keys) for licensing or operation.

5. All PSSP-EISS devices with a system clock must synchronize to the Primary Server network time using the Windows Time Service on the Network Time Protocol (NTP).

6. The PSSP-EISS must utilize at minimum Microsoft SQL Server 2012 database and must run in native mode.

7. The PSSP-EISS clients must operate Windows 10 operating system environment or newer.

8. The PSSP-EISS must operate in the Windows Server 2012 or newer operating system environment.

9. The PSSP-EISS must support unattended software and firmware installations and upgrades. In particular, all firmware must be downloadable without having to visit the panel location to perform an upgrade.

User Interface

10. It is required that the PSSP-EISS utilize an intuitive, industry-standard, Windows-compliant Graphical User Interface (GUI) for all administrative, user and configuration operations. It is required that the user interface provides an intuitive environment for the operational staff to manage functions, including monitoring and controlling system devices such as alarm sensors and door locks with an easy point-and-click method. It is also required that the user interface provides the familiar look-and-feel of current Windows based desktop environments by allowing the operator to view the system (and its operations) in a graphical format. It is required that a toolbar consisting of a collection of action-related icons be implemented to allow for easy system control. It is required that the system also provide comprehensive find, search and sort functions.

11. The PSSP-EISS must not require users to have Windows Administrator rights in order to launch, configure or use the application. The PSSP-EISS must require users to have Windows Administrator rights in order to install or upgrade the software.

12. It is desirable that the PSSP-EISS supports modules utilizing a web interface and integrates with Microsoft Internet Explorer, as well as Google Chrome for browser support to specific, widely used functions. Describe how the proposed PSSP-EISS supports these requirements.

IT Security

13. The PSSP-EISS must be deployed (and operate in) an IT security environment, the proposed system requires at a minimum the following:

    i. Each user must be uniquely identified. No network access to the PSSP-EISS resources and data must be permitted without the user being uniquely identified.
    ii. Passwords must be a minimum of 8 characters and should enforce the following characteristics: contain at least three of the four following elements: number, special character, upper case, lower case. The previous 8 passwords must not be reused.
    iii. The operator must be forced to sign-in at a PSSP-EISS workstation after 15 minutes of inactivity (client) and 15 minutes of inactivity (server). The Alarm Monitoring Workstation is to never lock and always be available for alarm response.
    iv. The PSSP-EISS must ensure that a record of all important security events and actions involving users and administrators must be maintained in protected audit logs.

14. The PSSP-EISS must use encrypted SMTP for all messaging communications over the network.

15. All PSSP-EISS databases must support data security mechanisms restricting unauthorized access and preventing tampering of stored data. These security mechanisms must ensure integrity, availability and confidentiality of the PSSP-EISS data.

16. Contingent and dependent on user privileges and workstation/server configuration, the user must have the capability of performing any data entry, alarm management, configuration and system management from any PSSP-EISS workstation on the network.

17. The PSSP-EISS must provide a role-based user permission facility. System administrators must have the ability to define users or groups of users to whom selective permissions are granted (e.g., particular applications, records – add/modify/delete). Users may be assigned to one or more groups. User groups must named groups consisting of users or groups of users.

18. The vendor or any contractor working on the system, using a device owned by GOC /GCnet or plugging into hardware (ex: switch) is prohibited from using any USB flash drives or external computers or laptops. If flash drives are required they are to be communicated to PS/SP, if accepted they must scanned by IT security PRIOR to being plugged in to any device(s) on the GOC network infrastructure.

Integration with Third Party Applications

19. The PSSP-EISS must be compatible with, at minimum, Microsoft Office 2013, including Outlook, Excel and Word.

20. The PSSP-EISS must be compatible with Adobe Acrobat Reader (V11 or later) for document viewing.

21. It is required that PSSP-EISS systems, modules, applications and components have a documented roadmap for supporting future versions of Microsoft products, operating system and databases for the next ten years. It is required that, at a minimum, it address Windows Server and Desktop Operating System, Microsoft SQL Server, Microsoft Internet Explorer, and PSSP-EISS application security and applications. Describe how the proposed PSSP-EISS supports this requirement.

Time Zone Support

22. The PSSP-EISS must support each standard time zone in the world and maintain the date/time integrity of all system configurations, transactions and reports derived from various future locations.

23. The PSSP-EISS must record, track and maintain the local time at the server, and the local time at each security panel (NTP server). The PSSP-EISS must manage each of these individual times such that alarms, events and transactions must be date/time stamped at their origin and such original date/time stamps must be maintained regardless of where they are reported or managed. Such time integrity must be maintained at all times.

24. It is desirable that the PSSP-EISS support the management of the system to support local/site specific Day Light Savings Times, where applicable. Describe how the proposed PSSP-EISS supports this requirement.

Connectivity

25. As the PSSP-EISS must communicate over a number of different physical network types, the PSSP-EISS must be tolerant to network packet loss, be able to recover from network outages and have a means of indicating to users that network conditions are impacting system performance. If network or power outages occur, each network-based controller must 'auto connect' on its own and must not require manual start up processes from an operator or user.

26. All PSSP-EISS subsystems must be Quality of Service (QoS) aware and support mapping to proper network QoS queues for multimedia and high priority traffic. Events and Alarms generated within and by the PSSP-EISS must receive the highest priority.

27. All PSSP-EISS systems and applications must use DHCP-assigned reserved addresses for the servers and nodes – not statically provisioned IP addresses (except where existing network equipment restricts such). Static IP addresses must be used for select security devices such as security panels. Servers should have the ability to manage DNS protocols.

28. The selected system must have the capability and include all software licencing to perform remote desktop application (RDP). It is desirable the system run in a Citrix environment. Citrix is not required to be implemented at this stage but for future requirements.

Active Directory

29. The PSSP-EISS must support a direct connection to a Microsoft Active Directory server. Active Directory integration must enable the synchronization of information from the Active Directory server to the PSSP-EISS servers.

30. When enabled, Active Directory must manage user logon to the PSSP-EISS client applications through the user's Windows credentials.

31. It must be possible to synchronize the following PSSP-EISS entities and their information from
    Active Directory to the PSSP-EISS:

    i. Users (username, first and last names, email address, and more)
    ii. User groups (user group name, description, and group email address)
    iii. Credential Holders (first and last names, description, email, and more)

32. It is required that, when enabled, the addition, removal, or suspension of a user's Windows account in Active Directory results in the creation, deletion, or disabling of the equivalent user account in the PSSP-EISS. Describe how the proposed PSSP-EISS supports this requirement.

33. It is required that, when enabled, the addition, removal, or suspension of a user's Windows account in Active Directory results in the creation, deletion, or disabling of the equivalent credential holder's account in the PSSP-EISS. Describe how the proposed PSSP-EISS supports this requirement.

SECTION E – STANDARDS COMPLIANCE

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must comply with the following standards: UL 294 – The Standard of Safety for Access Control System Units and UL 1076 – The Standard of Safety for Proprietary Alarm Units or CAN/ULC S319-05 – Electronic Access Control Systems and CAN/ULC S302-M91 (R1999) – Standard for Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults. Describe whether and how the proposed PSSP-EISS supports this requirement.

2. The PSSP-EISS must support approved encrypted communications between the servers and other servers; between the servers and workstations and between the servers and security panels. The application data and network traffic must be encrypted at AES 128 or better. Describe how the proposed PSSP-EISS supports these requirements.

3. The vendor must employ a quality management program in the development, manufacturing and support of its hardware and software products. It is desirable that the vendor possess an implemented quality management program (ie.: ISO Certification). Describe how this requirement is met.

4. The PSSP-EISS must incorporate network security and firewall policies as described in the Communications Security Establishment Canada (CSE) ITSG-22 Guideline. Describe how the proposed PSSP-EISS supports this requirement.

SECTION F – INTEGRATION

1. The PSSP-EISS must have integration with CCTV system(s) for future scalability. Describe what CCTV systems are best suited or may integrate (API / SDK) with the proposed system.

2. The PSSP-EISS has a mandate to install approx. 60 doors in the NCR (both sites listed), 40 doors for 269 Laurier & 20 doors for 340 Laurier. It is required the vendor provide all hardware/software and labour costs to integrate with the newly installed 60 automatic door operators at the time of installation which may be after hours work.

3. It is required for the PSSP-EISS to have the ability to perform a system wide (or area) 'Lockdown Event' for example in the event of an Active Shooter.

SECTION G – SCALABILITY

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must be designed and engineered to support future system growth, including adding access devices, alarm devices, cameras, workstations and servers without major hardware or software changes. The PSSP-EISS must have the ability to be gradually integrated to all of PS regional offices (list of locations in SECTION Q) and have the ability be managed and monitored from PS HQ in Ottawa, ON.

NOT as part of this phase, but for future expandability and usage of this contract, the bidder must be able to offer installation and service to our regional offices located in the cities that are listed in section Q.

2. The PSSP-EISS must be a scalable system with support for the following minimum number of security devices:

i. 2 system servers (one primary, one secondary)
    a. Master Primary – HQ;
    b. Master Secondary – 340 Laurier W.;

c. System Workstations x4;

ii. 12 users on 5 PSSP-EISS workstations or servers, with 5 simultaneously active at any time
iii. 200 security panels
iv. 1500 credential readers and/or keypads
v. 6000 alarm sensors
vi. 3500 relay output devices
vii. Local and Tech support for each standard time zone in Canada
viii. 25,000 credential holders

SECTION H – USER RIGHTS MANAGEMENT

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must support an unlimited number of system users, groups of users and passwords. The system must support the restriction of the capabilities of specific users or groups of users to only a group of defined functions. The PSSP-EISS must also allow the administrator to limit which users or groups may access specific credential records and panel as well as input or output records. The PSSP-EISS must provide a mechanism to synchronize the Active Directory users with the PSSP-EISS users, so that the addition and deletion of users requires no manual re-entry of data.

2. The PSSP-EISS must provide a facility for defining user rights to modules, functions and configuration capabilities Create, Read, Update and/or Delete:

i. Access Control Credentials
ii. Users
iii. Operators
iv. Alarms
v. Acknowledge Alarms
vi. Configure System Holiday Schedules
vii. Configure System Groups
viii. Configure PSSP-EISS Hardware
ix. Configure Network Hardware

x. Configure System Servers
xi. Create and Generate end user selectable reports.

SECTION I – SECURITY PANELS

1. The Security Panel provides the link between the PSSP-EISS Server and its hardware components such as credential readers, door locks, alarm sensors and output devices. Each Security Panel must possess all of the processing, memory and input/output facilities to

support each of its respective devices as described in Section I.5 below. The Security Panel must be based on micro-processor technology and offer completely autonomous operations. Upon system initiation, it must be possible to download all operating and credential holder data to the security panel from the PSSP-EISS Primary Server, or any Workstation. The failure of any security panel must not affect the operations of the other security panels in the network. Security panel software and firmware must be programmed in a high-level language for ease of maintenance and feature enhancement. Each main panel, sub-panel, and any other hardware are to be located in a centralized secure room per floor.

2. It is the vendor's responsibility to ensure that all necessary wiring/cabling, specialty equipment and tools, and all power supplies are adequate to support each installation. Should any issues arise it must be the vendor's responsibility, at their cost, to ensure proper functioning of the system.

3. All security panel operational code is stored in non-volatile ROM while system parameters and access control data is stored in battery-backed-up RAM. Each security panel must support downloadable software, using on-board Flash Memory. Flash downloads of new embedded software must be packaged and seamless.

4. Each security panel must contain an on-board, real-time, battery-backed-up clock for access control, event initiation, and date/time stamping of records. The security panel clock must be synchronized from the PSSP-EISS Site Server.

5. The security panel must support input voltage levels of approximately 120VAC, 60Hz and include appropriate switching power supplies and batteries to provide 8 hour operational battery backup in the event of AC power loss. The security panel must use common, industry-standard back-up batteries which would be generally commercially available. The security panel must report power loss or low battery conditions to the server. Each security panel must support an auto-restart capability for automatic start-up after power is applied. The security panel must automatically switch to battery-backup in the event of an AC power loss. Any electrical connections beyond what is already installed at each existing panel must be the responsibility of the vendor, and must have to be coordinated with the base building of each location. The client can assist in the coordination of the installations as required.

6. Each security panel on the PSSP-EISS must support a minimum of 25,000 credential holders, minimum 8 credential readers, minimum 12 alarm input points and 12 relay output points.

7. The PSSP-EISS must be capable of connecting to and managing Wiegand compatible card readers. The security panels and readers must support multiple facility codes.

8. The Security Panel must be capable of controlling access and reporting alarms simultaneously.

9. The Security Panel must support variable schedule-based door operations. For example, the PSSP-EISS (and Security Panel in off-line mode) must support reader only operation from 8:00 a.m. to 5:00 p.m. and reader/keypad from 5:00 p.m. to 8:00 a.m.

10. The Security Panel must continually communicate with the PSSP-EISS Server in order for it to report the receipt of an alarm condition, upload credential reads or receive changes in operating parameters or data. The Security Panel must be capable of operating in a standalone fashion such that all access control decisions are made based on the verification of an individual credential against access control parameters and data stored at the Security Panel. Such verification must include credential ID, time of day, and facility code at all times, even if in stand-alone mode. Degraded non-facility code checks are not acceptable.

11. The PSSP-EISS Security Panel must communicate via 10/100/1000 MB Ethernet and must have the capability of residing on a local area network (LAN) or a wide area network (WAN) without connectivity to a computer serial port.

12. The Security Panel must support 10/100/1000 MB Ethernet connection to the PSSP-EISS Server. Downstream devices off the security panel may be RS-485 or equivalent if required.

13. It is desirable that a complete initialization and download of the Security Panel operating instructions and credential holder database (at 25,000 credential holders) not take longer than 5 minutes when connected via 10/100 MB Ethernet. Describe how the proposed PSSP-EISS supports this requirement.

14. The Security Panel must contain Light Emitting Diodes (LEDs), which display both transmit and receive status from the PSSP-EISS Local Server. LEDs must also provide status on power supplied directly or via the battery back-up system.

15. All system operating data must be stored in the PSSP-EISS Primary and Secondary Master Servers and must be automatically downloaded to the Security Panel once saved in the PSSP-EISS database. All database changes (e.g., credential holder adds/deletes/modifies) must be sent in an encrypted manner to the security panels in real time when any pertinent data element is changed.

16. It must be possible to define the local time at each regional office or facility. Such time must be applied to each security panel and PSSP-EISS workstation in the facility. The time of all access and user transactions, alarms, events and output activations, for example, must be date and time stamped to the local time at the office or facility. The server must receive such transactions and retain the local date and time stamp from the data received from the office or facility's devices (e.g., security panel).

17. The response time from a valid credential presentation to a successful access granted at the door or portal must be less than one second. All access requests must be processed locally in the Security Panel.

18. All security panels and sub-modules must be housed in locked, tamper-proof enclosures restricting access or accidental damage and contain and have operational tamper switches.

19. Each PSSP-EISS security panel must be capable of operating autonomously without a network connection. During autonomous operation, the security panels must retain full functionality (with the exception of alarm display at a PSSP-EISS workstation) using locally stored access control data and must retain all access control and alarm transactions. Transactional information (including alarm data) must be retrieved by the PSSP-EISS Server when the network connection is restored. The PSSP-EISS must store a minimum of 5,000 access transactions and 5,000 alarms/events, at a minimum, before overwriting the oldest events.

20. Security panel specific alarms must be defined for AC power loss, communications errors and security panel cabinet tamper.

21. It must be possible to purchase controllers, modules, power supplies and other equipment integral to the security panels (without chassis) from the Vendor.

22. Security panel warranties must be maintained regardless of existing or new mounting and configuration methods provided that installation guidelines are followed

23. The PSSP-EISS must support the use of End-of-Line resistors to monitor for line tamper conditions. The PSSP-EISS must support one, and two end-of-line resistor configurations on a single pair of wires serving one or two devices. The PSSP-EISS must support resistor modules to provide such supervision such as 'open, close, cut and short' conditions.

24. It is desirable for the operating and storage requirements of the security panel to be:

    i. Storage Temperature: 0°C to 50°C
    ii. Storage Relative Humidity: 0 to 95% R.H. (non-condensing)
    iii. Operating Temperature: 0°C to 50°C
    iv. Operating Relative Humidity: 0 to 80% R.H. (non-condensing)

25. It is desirable for the security panel to utilize fire-retardant epoxy in its printed circuit boards and UL/CSA-rated components, where applicable.

    It is desirable for each security panel to:

    i. comply with the United States FCC, Part 15, Subpart B, Class A rules,
    ii. comply with the Council Directive 73/23/EEC CSA 22.2 950
    iii. have CSA NRTLC/C designation and meet Canadian and USA safety standards
    iv. be CE marked.

SECTION J – ACCESS CONTROL

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must provide fully-featured, distributed access control capabilities. The PSSP-EISS must utilize servers and workstations, security panels and electronic credential readers for defining user access parameters and controlling access to buildings and areas.

2. All standard access control configuration and storage functions must be provided from the PSSP-EISS Master Servers, as well as PSSP-EISS workstations. Such functions must include, but not limited to:
    i. Entry of access control configuration data
    ii. Entry of access control operating data
    iii. Storage and display of access control data
    iv. Downloading of user status data to the security panel(s)
    v. Editing of access control data
    vi. Archiving of access transactions
    vii. Retrieval of access records from the security panel(s)
    viii. Editing/display of credential holder status
    ix. Integration of access control module to other PSSP-EISS modules
    x. Generation of management and archive/transaction reports
    xi. Map/Floor plan integration

3. The PSSP-EISS must support up to 25,000 credential holders

4. The PSSP-EISS must support the access management of a number of different portal types, including but not limited to: single and double access doors, handicap actuated/assisted doors* see , airlocks, turnstiles, overhead doors, vehicular gates, and elevators.

5. Each security panel must support a minimum of 8 credential readers. These readers must be capable of reading the internal data encoded into each card (or the credential) then send this information to the security panel. The security panel must process this information and unlock the appropriate controlled portal only if the credential is determined to be valid.

6. It must be possible to configure a PSSP-EISS portal for credential reading IN only, and IN and OUT.

7. The PSSP-EISS must support the credential readers which are deployed on the same system as well as the same security panel. The PSSP-EISS must support the following credential readers:
    i. HID Wiegand compatible readers with 26 bit standard Wiegand data format
    ii. HID iClass/Seos or similar smart card capabilities for future expansion

Describe how the proposed PSSP-EISS supports this requirement.

8. The PSSP-EISS must support the definition of a credential holder with, at a minimum, the following fields or attributes:

    i. Salutation (i.e., Dr., Miss., Mr., Mrs., Ms., Prof.)
    ii. First Name
    iii. Middle Name or Initial (optional)
    iv. Last Name
    v. Position
    vi. Division
    vii. Type (e.g., Indeterminate, Term, Casual, Student, Contractor, Visitor, Other, etc.)
    viii. Direct Dial No.
    ix. Cell No.
    x. Internal Card Number
    xi. External Card Number (if different)
    xii. PIN (hidden and/or visible)
    xiii. Card Serial Number (if Smart Card implementation)
    xiv. Activation Date
    xv. Expiration Date
    xvi. Status
    xvii. Access Group
    xviii. Photo
    xix. Photo Identification Badge Template
    xx. Signature
    xxi. A minimum of 10 additional User Definable Fields
    xxii. Profile Modification Date / User and Workstation Identification

9. As the volume of credential changes may be very high, it is desirable for the PSSP-EISS to provide an intuitive, effective and efficient means of creating, reading, updating and deleting credential records. Describe how the proposed PSSP-EISS supports this requirement.

10. The PSSP-EISS must support a minimum of 4-digit PINs that are auto generated by the PSSP-EISS (and not user selectable). The PINs must be encrypted in the database and their transmission to the security panels must be encrypted.

11. The PSSP-EISS must support the ability for users with the appropriate permissions to query and view credential holder information from any PSSP-EISS workstation. Such information must include all static and user-defined fields in the credential holder record.

12. It must not be possible for a system administrator or operator to view the credential holder's PIN unless so authorized, access to which must be strictly limited.

13. The PSSP-EISS must generate, report and display alarms associated with invalid access attempts (e.g., wrong time schedule, invalid credential, no access at that reader/keypad, etc.).

14. The response time from card (or credential) read to door unlock must be less than one second. All access requests must be processed locally in the security panel for faster response. Additionally, the door held open time limit and door unlock time-out must be user-adjustable with a time span ranging from 1 to 255 seconds.

15. Each security panel must be capable of supporting fully supervised exit switches that are associated with each reader-controlled door. Activation of an exit switch (either pushbutton, passive infrared, or panic bar) must release the locking device and allow the door to open. Normal access control, time-out logic must follow exit switch activation. Each exit switch input must be capable of being configured, via software, to shunt the associated alarm or shunt the associated alarm and unlock the door. When the exit switch is used, the associated door contact must be de-bounced in order to prevent false alarms.

16. If a security panel determines that a credential holder is not to be granted access through one of its associated doors, the door must remain locked and an invalid credential alarm must be generated.

17. The PSSP-EISS must support an anti-passback feature such that the system prevents repeated use of a credential at the same door. It is also desirable for hard, soft and timed anti-passback to be supported.
    i. Hard anti-passback is defined as a software configuration which disallows the use of a valid credential at an “IN” reader unless it has been used at the corresponding “OUT” reader.
    ii. Soft anti-passback is defined as a software configuration which allows the use of a valid credential at an “IN” reader without it having been used at the corresponding “OUT” reader, but presents an alarm event upon such an occurrence.
    iii. Timed anti-passback is defined as a software configuration which disallows the use of a valid credential at a reader unless a certain period of time has passed since it was last used at the same reader.

18. The PSSP-EISS is to provide a facility for the creation and definition of access groups which defines to which readers the credential holder (or group of holders) has access authority, at which times of day and days of the week (or holidays). Credential holders may be grouped together within access groups. Readers/keypads may be grouped together into access groups. It is desirable that the capability to assign multiple time schedules to an access group be possible. Describe how the proposed PSSP-EISS supports this requirement.

19. For access control purposes, the system must support an unlimited number of holiday groups, each of which may contain up to 32 holidays. It is desirable that a holiday be defined in terms of start-day and stop-day. Holidays may be configured as day-of-year, day-

of-month, day-of-week, and combinations thereof, as well as discrete date ranges. Each Holiday Group and Holiday are to carry a name of up to 32 characters. The capability to configure holidays and holiday groups as recurring events (weekly, monthly or annually) must be possible and holiday events are to be location-specific and not system-wide. As such, holidays may be configured for one location and not affect those configured for another location. Describe how the proposed PSSP-EISS supports these requirements.

20. The PSSP-EISS must allow support for the definition of access groups with, at a minimum, the following fields or attributes:
    i. Access Group Name
    ii. Readers and/or zones
    iii. Time schedules

21. The PSSP-EISS must support the following advanced access control features:
    i. Access groups
    ii. Schedules
    iii. Holidays
    iv. Escort requirements
    v. Handicap operation rules/extended operation
    vi. Automatic credential expiry (date, or number of uses)

22. The PSSP-EISS must support the creation and definition of an unlimited number of temporary access groups. Describe how the proposed PSSP-EISS supports this requirement.

23. In order to simplify the amount of data entry and effort required in the administration of the PSSP-EISS system, the software is to provide a behaviour-based method of programming the access rights for each credential holder. It is requested that the PSSP-EISS operate as follows:
    i. Credential readers grouped into Zones, which are given names to conform to their real-world counterparts (e.g. Perimeter Doors, Operational Zone, Security Zone, and High Security Zone).
    ii. Zones and Time Schedules combined in pairs to define a logical concept referred to as an Access Group. *Essentially, an Access Group represents a number of Access Zones and Time Schedules. The ability to name an Access Group (e.g. Employees, Contractors, Locally Engaged Staff etc.) allows for the Access Group to be referred to in conventional terms that are familiar to all users of the system, and which are in everyday use.*
    iii. By assigning each credential holder to the appropriate Access Group, the system automatically grants that credential holder's access rights to all of the Access Zones/Time Schedule pairs defined for that Access Group.

24. It is required of the system to support an additional facility to allow for exceptions to be applied to any credential holder or access group such that new access groups need not be developed for single or a small number of exceptions (i.e., an individual credential holder

with access to a standard zone but restricted to NOT access a particular area within that zone). Exceptions can be based on the particular zones included in the access group, as well as the time schedules of operation for each particular zone. Describe how the proposed PSSP-EISS supports this requirement.

Note: if the vendor does not provide an “exception” facility, it is desirable for the vendor to describe how the proposed system allows for such functionality in a different manner thus eliminating the need for additional access groups to be defined for single (or a small number of) credential holders with specific access requirements.

25. It is required for the PSSP-EISS to support the following capacities of Access Groups, Access Zones and Time Schedules:
    i. Access Groups: unlimited
    ii. Access Zones: unlimited
    iii. Time Schedules: unlimited

26. The PSSP-EISS must support the creation and definition of an unlimited number of role-based access groups and schedules which are associated with credential holders and areas or zones for which the credential holder is granted access privileges.

27. The PSSP-EISS is to provide a facility for expiring a credential on a certain date and at a certain time. In addition, it is desirable for the system to provide a feature to allow for the definition of a specific number of times a credential may be used. Such definition must range from 1-999 times from its first use (including the first time it is used). As well, the system is to provide a facility to define the number of days from its first use or from the date of activation (either of which may be selected) during which time the credential must remain active. Such settings must range from 1-999 days. Describe how the proposed PSSP-EISS supports these requirements.

28. The PSSP-EISS is to provide a number of usability features such as auto populate, pull-down menu items, label customization, window layout configuration, filters, partial entry and multi-field search facilities, and pre-populated fields for ease of data management and efficiency of system administration. Describe how the proposed PSSP-EISS supports this requirement.

29. The PSSP-EISS must support the bulk loading of credential holder data (including photos) from external or existing systems or databases. The system must provide tools to support such database loading. If no tools are available, manual transfer of data must be the responsibility of the vendor.

30. It is required that the PSSP-EISS provide an escort feature whereby certain credential holders may be defined as "requiring escort" and other credential holders may be defined as "escorts". When so configured, it is desirable for a credential designated as "requiring escort" to be presented to a reader at which time the reader must expect the escort to

present a credential to the same reader. Once authorized, the door or portal must be unlocked. It is desirable for such feature to be assignable to any or all readers in the system and may be enabled for a particular time using the same time schedule facility used elsewhere in the system. For ease of data entry, it is desirable that the system default to "standard" credential holder such that any credential holder requiring escort or being defined as an escort must require a discrete change to the default. Describe how the proposed PSSP-EISS supports these requirements.

31. The PSSP-EISS must support an “extended operation” feature whereby the administrator may modify the default door unlock and door held times for credentials designated as “Extended Operation”. Such feature must be utilized on handicap assist doors or portals. When an authorized credential designated as “extended operation” is used at a particular reader, if so configured, the door must open automatically, if equipped with an operator assist device, and the extended door held and door unlock times must be invoked. Such operation may also be applied to a time schedule.

32. The PSSP-EISS must support the storage of all access control and intrusion alarm monitoring transaction data, events and alarms for a minimum of 2 years. Such events must be stored in each of the Master Servers.

SECTION K – PHOTO IDENTIFICATION MANAGEMENT

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must support a fully integrated photo identification badge creation, management and production facility. The PSSP-EISS Photo Identification Management subsystem must be a fully integrated software and hardware solution for the capture and storage of high resolution digitized photo images. By virtue of the integrated database, all data entered into the employee database must be immediately available at any PSSP-EISS workstation.

2. The PSSP-EISS must support industry standard photograph capture cameras, card printers, USB signature tablets and all associated peripheral devices required for a fully functioning photo identification management subsystem.

3. All information included in the credential holder record must be fully integrated with the photo identification facility. The high-resolution video images must be captured, digitized and stored on the local hard disk at the PSSP-EISS workstation equipped for the capture and enrollment of credential holders with photographs. Once the image has been captured, it must be treated as part of the PSSP-EISS database stored in the Primary and Secondary Servers and may be called up for visual ID confirmation at any other PSSP-EISS workstation equipped with a video imaging module, or used for badge production and printing. Any PSSP-EISS workstation must be able to view credential holder photos without requiring special hardware.

4. The PSSP-EISS must support the creation, management, update and archiving of multiple photo identification design templates. The photo identification design tool must support photograph and signature image management, be fully integrated with the access control database, provide industry-standard drawing tools and elements, allow for the insert/importing of industry-standard-format images, allow for the management of aspect ratios and image cropping and support multiple templates/designs per credential holder. The badge must be designed in a fully interactive mode, with a real-time display of its current form during the process. It must also be drawn using the high-resolution mode of the video display module, for maximum accuracy and faithful reproduction of finished badges. Each new badge template must be stored for rapid retrieval and application, during user badge production. The completed badges must be available for high resolution viewing at any time.

5. The PSSP-EISS must support photo identification badge design facility that includes standard graphic design tools (lines, boxes, circles, etc.), multiple line and fill patterns and colours, user controlled picture sizes and aspect ratios, front views/side views and signature captures, access to all database fields, standard Windows fonts, static graphics, user controlled object stacking, database conditional fields, various colours, other security features (e.g., holograms), signatures, barcodes, 2-sided printing and crop-to-fit features. It is also required for the PSSP-EISS to support a feature whereby the aspect ratio associated with the photo capture window is locked for each badge template. It is required for the system to also provide a “crop-to-fit” feature to support the ability to add photos from an existing photo database and crop the photo to fit the aspect ratio on the new badge template. Describe how the proposed PSSP-EISS supports each of these requirements.

6. The PSSP-EISS must be required to support the existing badge printer and camera hardware models:

    - HID HDP5600 Printer
    - Logitech C920 1080P HD Web Camera

SECTION L – ALARM MONITORING AND CONTROL

1. Alarms must be reported and displayed on either a graphic floor plan or in a list at the pre-defined Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) workstation within 2 seconds from the time the sensor is triggered.

2. The PSSP-EISS must support the connection of a variety of supervised alarm input devices such as door position switches (door contacts), motion detectors, glass break detectors, duress buttons and similar signaling devices.

3. For PSSP-EISS Operator Workstations configured to receive and process alarms, the system must, upon receipt of an alarm, perform the following:

    i. Display the alarm(s) and activate a sound to which the guard must respond
    ii. Display in colour, a graphic floor plan of the area from where the alarm(s) originates, or if the operator chooses, present the alarm(s) in a list format. Alarms must be displayed in order of priority
    iii. Display the name of the floor plan associated with the point that is being reported. The display must use colour-coded icons, superimposed on the floor plan, to indicate the actual location of the alarm. Distinct and different colours must represent the following: alarm state, tamper or failed state, disabled state or secure state. The colours must be user-definable
    iv. Display a full description of the alarm and state of the alarm point
    v. Display the date and time that the alarm point first reported
    vi. Archive the alarm event information including, its state and the date and time of the occurrence on the Primary and Secondary Master Servers
    vii. Send the technical information and alarm to mobile device(s), if applicable
    viii. Send the technical information and alarm to the system dialer, if applicable
    ix. The annunciation of alarms must take precedence over any other tasks being performed; such tasks must be suspended until the alarm processing is complete and must then be restored at the point of interruption
    x. If the alarm is a credential-related event, and a photo has been stored for that credential holder, a button in the tool bar must prompt for a window which must display the credential holder's photo, name and ID number, as well as the last reader accessed by that credential holder
    xi. In the event of a duress alarm, such alarm must be of highest priority and must also be displayed at the Identification Management Workstation.

4. At a minimum, it must be possible to define, configure and program the following attributes for each alarm/event input:
    i. Alarm/Event Technical Address: The alarm point information must be indicated in a form, which describes the security panel number, type, module type and name or input number.
    ii. Alarm/Event Description: The system must allow a description to be associated with each alarm.
    iii. Alarm Priority: Alarms must be assigned a user-definable priority number (from 1 to 16) to distinguish their relative importance in the event of multiple alarms occurring simultaneously.
    iv. Display Group System users must have the capability of designating which PSSP-EISS workstation or group of PSSP-EISS workstations must receive and display which alarm conditions. Up to 16 groups of reporting stations must be designated with multiple PSSP-EISS workstations capable of being assigned to each reporting group. A group must be defined as any set of PSSP-EISS

workstations on the network. It must be possible to route alarms to display groups, regardless of user profiles or log-in privileges.

v. Camera Action Definition: The system must be capable to link an alarm input to a CCTV camera input popup with their associated PTZ preset positions depending on camera compatibility. Thus, upon occurrence of an alarm condition, the PSSP-EISS system must be activated such that visual supervision can be established for the detection zone.

vi. Instruction Set or Individual Instruction: Each alarm point must be capable of being associated with an instruction set such that upon occurrence of an alarm condition, the system operator must have the ability to call it up. It must be possible to create and edit these instruction sets from any PSSP-EISS workstation on the network, given the operator has the proper authority level. Reports on these events must be required to be generated through the PSSP-EISS.

vii. Input Icon Type and Colour: The system must allow various icons to be associated with alarm points. When the icon is being selected to be applied to an alarm point, it must be displayed graphically.

viii. Floor Plan: The system must provide, as a standard feature, a high resolution graphics facility for displaying colour floor plans/maps in order to assist operators in locating and responding to alarm conditions.

ix. Linked Outputs: For each alarm point, users must be able to link relays for equipment control. For each alarm point the options of linked actions must include: latch the relay on and then have the operator reset it from the central site; have the relay automatically follow the alarm status, or pulse the relay for a specified period of time after a change of state of the alarm point.

x. Linked Programs or Actions: For each alarm point, users must be able to link programs and actions when integrated with third party applications and CCTV applications.

xi. Schedule: The system must provide a minimum of 128 time schedules. Each alarm point may be assigned to any one of these schedules for automatic shunting.

xii. Alarm Group: An alarm group can be a combination of inputs. The groups must be presented to the operator as a single icon to allow the operator to carry out actions for the entire group as a single function. The operator must also be able to manipulate individual members of the group.

xiii. Alarm Sound: It must be possible to define a unique alarm sound via a .wav file for each alarm input. The system must be delivered with a default computer-generated sound.

xiv. Manual Control: While in manual control the system must allow a user to reverse the existing state of an input, a relay or a local group.

5. It is required for the PSSP-EISS to provide an alarm management and display capability for reporting and displaying alarms at one or more PSSP-EISS workstations. Upon displaying the alarm, the following information, at a minimum, is to be provided:

i. alarm type (illustrated with an icon – e.g., door position switch, motion detector, duress alarm)
ii. date and time of alarm (local to that security panel)
iii. alarm description (in plain language)
iv. technical details associated with the alarm (technical address)
v. displaying alarm on a floor plan or in a list view (configurable)
vi. operator sound alerting (customizable by alarm)
vii. additional information or actions integration with the alarm or called up by the operator (such as video, audio, photo of the individual associated with the credential, etc.)
viii. automatically generated messaging (e-mail and/or SMS) alert (which may contain a subset of the above information)

6. It is desirable for the PSSP-EISS to support the reporting and display of alarm events on external display (mobile) devices such as, smartphones and cellular telephones. For such alarms, it is desirable that the PSSP-EISS provide the following information in its message to the mobile device:
    i. alarm type
    ii. date and time of alarm (local to that security panel)
    iii. alarm description (in plain language)
    iv. technical details associated with the alarm (technical address)
    v. integrated audible alert

    If the proposed system supports this feature, describe how the proposed PSSP-EISS supports this requirement.

7. For each alarm and/or event in the PSSP-EISS, it must be possible to define its name, alarm group, priority, archive action, instruction set, floor plan, icon, schedule, ability to control the alarm manually (i.e., can it be shunted), location for its display upon occurrence, camera program, linked outputs, alarm sounds, dialer/email destination groups.

8. It must be possible to report alarms to multiple locations (or destinations) simultaneously or sequentially, based on the alarm type or time schedule.

9. It must be possible for the PSSP-EISS to support the use of floor plans for displaying alarm occurrences. A floor plan must be automatically displayed on the screen with each alarm occurrence provided that it has been previously specified to utilize that graphics-based display. The system must support a mouse-driven drop-and-place alarm icon placement function. Once the alarm icon has been placed onto the map, the system administrator may select it and place it anywhere on the plan. The PSSP-EISS must support the import of graphic floor plans in .bmp or .jpg format. The PSSP-EISS must support the addition of the noted device icons as separate entities on the floor plans.

10. The PSSP-EISS must provide a facility for defining how an alarm is acknowledged and cleared
    - either by a particular user, a user group or PSSP-EISS workstation or PSSP-EISS workstation group, or both/all.

11. It is required that the system supports a feature whereby alarm inputs may be logically gathered into “alarm groups”. Each alarm group must then be represented in the system by a single icon which may be expanded to show its elements. It is required for the operator to still have access to controlling each element of the group and that such a facility be used for implementing zoning strategies. Describe how the proposed PSSP-EISS supports this requirement.

12. The PSSP-EISS must support a facility for the activation of security postures wherein particular zones are automatically locked down, armed, disarmed or similar actions. Describe how the proposed PSSP-EISS supports this requirement.

13. It must be possible to link any output in the system to the activation of any input in the system such that upon activation of the input, the output relay either latches, pulses or follows the state of the alarm input.

14. Any PSSP-EISS administrator must have the ability to manually select and control any relay output in the system. Once the icon representing the output has been selected, a control window pops up and the operator may activate the relay output for a user-definable time period.

15. The system must provide for the capability of linking an alarm input point to a digital output point. It must be possible to designate this output point to either latch, pulse, or follow the state of the alarm input point. When latching, the digital output point must change state and remain that way until changed by operator command. In pulse mode, the relay must be energized for a user-definable period (0 to 8,000 seconds). In follow mode, the digital output point changes state as the alarm input point changes state.

16. Each digital output point may be assigned to time schedules such that the states of the relays change during the assigned time period. This feature must be utilized for automatically controlling elevators, doors, lights, gates and other equipment.

17. It must be possible for the administrator to manually override or lock a relay in a specified state, thus preventing it from changing state again until manually unlocked regardless of time schedule assignment or alarm linkages in effect.

18. It must be possible for a PSSP-EISS administrator to define an output point, such that each manual operation of that output point must be acknowledged with an “action reason” by the PSSP-EISS operator before it reacts. Describe how the proposed PSSP-EISS supports this requirement.

19. The system must support a Local Alarm Control capability for arming/disarming zones based on in-zone keypads. Zones may be armed/disarmed locally or armed from any PSSP-EISS workstation on the network, as so authorized. It is required that the keypad be based on an industry standard matrix keypad with display. It is also required for the system to support the configuration of inputs into zones to be controlled by the in-zone keypad or any PSSP-EISS workstation on the network. It is also required for the system to automatically synchronize the local alarm input configurations between the local alarm configuration and the PSSP-EISS database. The keypad must display all open zones, system status, trouble conditions and provide an audible notification for arming/disarming the zone. The system must also support auto arming schedules. Additionally, all actions are to be archived and date and time stamped. Describe how the proposed PSSP-EISS supports these requirements.

SECTION M – VIDEO MANAGEMENT

1. At this time it is NOT required that any existing Video Management Software (VMS) be integrated to the PSSP-EISS, however the PSSP-EISS must be capable of seamless video integration. No existing CCTV hardware and software is to be replaced but must require service coverage in the service contract (Section – S)

SECTION N – MANAGEMENT REPORTING

1. The Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) must support the real-time archiving of all historical data: access transactions, alarm events, video images, system activity, operator and administrator activity, data management actions and configuration modifications.

2. The PSSP-EISS must support a flexible reporting package to allow for the generation of report data. The report functions must allow for the quick and easy selection of various fields, using drop down menus. It must allow for common requirements and custom report generation facilities that are configurable by the user.

3. Reports must be activated in one or more of the following ways:
    i. Operator Initiated (Manual)
    ii. Periodic activation at user specified intervals
    iii. Application Initiated

4. The PSSP-EISS must provide a flexible method for on-line, real-time data queries from anywhere within the PSSP-EISS application.

5. The PSSP-EISS must provide an alert to the system administrator should its capacity be limited and archiving of all transactions and data be in jeopardy.

6. All PSSP-EISS reports must be stored in the system database and must be able to be viewed from any PSSP-EISS Operator or Administrator workstation and be controlled via system permissions. As data is generated in and from many different time zones, the system must display events and activities in the reports based on their local time and that time archived in the system transaction database. The PSSP-EISS must allow the user to export reports based on system events or on a user-defined schedule.

7. The PSSP-EISS must provide database and archive/transaction reports. The system must be delivered with a number of standard database and archive/transaction reports, which cover the most commonly-requested information.

8. Configuration of Management Reports must only require entry of the schedule information, and other parameters such as Credential Holder(s), Alarm/Event Name(s), filter information or time interval for search to fully configure the report. No programming or scripting must be required.

9. It is required that the PSSP-EISS be delivered with the following standard reports available in the system:
    i. System Users and Privileges
    ii. Administrators
    iii. Operators
    iv. Technical Staff
    v. Credential Holders (including all, or a subset of all, fields in each record)
    vi. Access Groups, Levels
    vii. System Event Transactions
    viii. Valid, invalid access attempts
    ix. Alarms/Events, including acknowledgement and responses
    x. Anti-passback activities and violations
    xi. Alarm/Video Linked Events
    xii. Scheduled Events
    xiii. System Hardware
    xiv. Servers, Workstations
    xv. Security Panels
    xvi. Security Panel Modules
    xvii. Readers, Doors, Portals
    xviii. Alarm Inputs
    xix. Relay Outputs
    xx. Cameras
    xxi. System Configurations
    xxii. Access Groups, Levels
    xxiii. Alarm Groups and Zones
    xxiv. Holidays, Schedules
    xxv. Anti-Passback Configurations

10. Describe how the proposed PSSP-EISS supports these requirements.

11. It is required of the PSSP-EISS to manually and automatically export (or send to a drive location) reports in each of the following formats: .pdf, .txt, .doc, .xls. Describe how the proposed PSSP-EISS supports this requirement.

12. It is required of the PSSP-EISS to provide a database change audit capability. For each field change in the database, it is desirable for the system to archive and display, in real time (and allow for future reporting), the change date, login name, table name, context, type of change (insert, modify, delete), field name, old value, old context, new value, and new context. It is desirable for all changes to be date and time stamped to the second. Describe how the proposed PSSP-EISS supports this requirement.

13. It is required for the PSSP-EISS to provide Admin users with the capabilities to review and trace all generated reports on the system.

SECTION O – DOCUMENTATION

1. The following Public Safety / Sécurité publique – Enterprise Integrated Security System (PSSP-EISS) documentation must be provided at the time of proposal submission, electronically and hard copy, in English language only, PS/SP will arrange for the translation of Contractor-produced deliverables, as required.

    i. Configuration Manuals: The Configuration Manuals must include descriptions related to the Access Control and CCTV platforms and their technical configuration parameters with particular emphasis on the Master Primary and Secondary servers, NVRs and Appliances, security panel software, hardware and networking parameters and installation procedures. At a minimum, such manuals must address the PSSP-EISS servers, PSSP-EISS workstations, operating system, network, database, port definition and management, service operation, communications, security panel modules, video system cameras and storage devices and implementation of the PSSP-EISS head end components.

    ii. Operator Manuals: The Operator Manuals must include descriptions related to the operation of the system with particular emphasis on alarm monitoring, reporting and management as well as integrated system functionality typically performed by system operators (e.g., guards, surveillance teams). At a minimum, such manuals must address PSSP-EISS workstations, system start-up and logon procedures, system shut-down and logoff procedures, use the system and its associated commands and software, alarm monitoring and management, video monitoring and surveillance, integrated system functionality, report generation, data entry, operator navigational commands, alarm descriptions and actions and system security requirements.

    iii. Administrator Manuals: The Administrator Manuals must include descriptions of the functions of all software modules and must include all other information required to effectively and efficiently manage the PSSP-EISS. The Administrator Manual must address the configuration and management of the PSSP-EISS application software and each of its respective modules. At a minimum, the Administrator Manual must provide an overview of the PSSP-EISS application, a review of all common user interface tools (e.g., add/delete/modify data, search and find functions, data views and filters, toolbars and menus) and assistance in planning the system parameters. At a minimum, the Administrator Manual must address: PSSP-EISS application user profiles, access control privileges and parameters, credential holder database management, access groups, schedules, zones, credential holders, alarm system definitions, video system management parameters, visitor management system configuration and programming, photo identification system configuration and

programming, subsystem integration (e.g., Active Directory), and archiving and management reporting.

iv. Installation Manuals: The Installation Manuals must include descriptions on the proper and best practice methods for the installation of Vendor hardware products and associated field devices and components, including the establishment of communication channels. At a minimum, such manuals must provide a general description of the system, 'As built' drawings, hardware and components and address installation procedures, equipment layout and electrical schematics, power requirements, system layout and schematics, and repair and replacement parts.

v. Maintenance Manuals: The Maintenance Manuals must include descriptions of the maintenance, support, troubleshooting and service instructions for all equipment and applicable software modules. At a minimum, such manuals must address inspection, preventative maintenance, fault diagnostics, repair and replacement procedures.

2. In addition, the PSSP-EISS must contain an online context-sensitive help facility to support PSSP-EISS users in the configuration and operation of the PSSP-EISS. The help menus must be available from any window in the PSSP-EISS by clicking on an icon that is always present in the same screen position or by pressing a specific function key. Help windows must be context sensitive so system users can move from the different operating windows without leaving the help window. Standard windows help commands for Contents, Search, Back, and Print must also be available.

3. As part of its submission, the Vendor is also to provide a separate copy of the complete on-line documentation files in a readily accessible electronic format such as .pdf or .doc files. Describe how the vendor supports this requirement.

4. It is required that the PSSP-EISS vendor provide access to their support tools and mechanisms, including but not limited to: release notes, technical notes, engineering change notices, bug lists, outstanding issues lists, on-line support forums, user groups and mechanisms for requesting features and new capabilities. Describe how the vendor supports this requirement.

SECTION P – MASTER PARTS LIST

Vendors must:

1. Provide a Master Parts List of all components, including third party components that would be required to deliver a complete Public Safety Canada - Enterprise Integrated Security System (PSSP-EISS) using vendor and third party components and software.

2. The Master Parts List must include all items listed in section R.

3. The Master Parts List must include additional parts, as required, for a fully functional PSSP-EISS.

4. Note that detailed requirements are not provided for security devices such as door position switches, alarm sensors, door locks, piezo sounders, etc. Such products may be proposed by the vendor to support a complete PSSP-EISS implementation.

5. The PSSP-EISS system must be compatible with, and support, the products listed in section R.

SECTION Q – VENDOR RESOURCES

PS/SP will require the support of vendor resources during various installation phases of the system implementation. The vendor must provide a minimum of one compliant resource in each of the resource categories included in this section.

It is required that the vendor offer in the proposal an option for a guaranteed 4-hour response time for all (2) sites located in the National Capital Region.

The vendor must provide contact information for each of the resources for each location mentioned, unless otherwise stated during the work execution with minimum notice of 24h of who will be working and where the work will take place. Each resource must be a direct employee of the vendor, no third party companies are to be used unless they are special trades such as electricians and locksmiths. Each resource must include, at a minimum: full name, work location, security clearance level and file numbers, project and role descriptions, industry and product certifications (including certifications on the proposed product).

The vendor must provide resources that meet or exceed the requirements as follows:

1. **System Architect**: A subject matter expert with extensive knowledge and experience with the system and designing core infrastructure. Security cleared to **RELIABILITY**.

2. **Project Manager**: A project manager with extensive experience in the work breakdown structure and process of designing and implementing a new core system implementation and transitioning from an existing system. Security cleared to **RELIABILITY**.

3. **Hardware Technician**: A technician with extensive experience and skill in implementing, testing and fine tuning new core system hardware and software. Security cleared to **RELIABILITY**.

4. **Application Software Technician Authority**: An application software technical authority with experience and skill in implementing, testing and fine turning the applications and third party software for the core system and user stations. Security cleared to **RELIABILITY**.

5. **Trainer (NCR Only)** : A bilingual (Canadian French and English) trainer with experience subject matter expertise and experience in training system administrators, operators, installers and maintainers of the PSSP-EISS. Bilingual means having written and verbal fluency in both languages. Demonstrate using specific teaching certificates or manufacturer accreditations and years of experience. At this time the PS/SP requires a minimum of (6) employees trained on how to use the system. Security cleared to **RELIABILITY**.

The vendor must be required to offer all services required in this document to the following locations;

- Burnaby, BC
- Edmonton, AB
- Regina, SK
- Winnipeg, MB
- Fredericton, NB
- Toronto, ON
- Ottawa, ON
- Montreal, QC
- Dartmouth, NS
- Charlottetown, PEI
- St. John's, NL

SECTION R –DEPARTMENTAL SITES & HARDWARE REQUIREMENTS

In order for to facilitate the vendor's proposal, the following is a brief description of each site's hardware requirements. Components that are already installed are expected to remain unless specified and must integrate and function with parts of or all of the proposed system are also indicated.

Important Note: The vendor must be responsible for the coordination, installation, hardware supply, programming, testing, and commissioning of both sites indicated below.

1. 269 Laurier Ave, Ottawa, Ontario – HQ and Security Operations Centre, comprised of up to 13 floors.

Existing;

- 247 Card Readers and associated door hardware
- 90 Intrusion Keypads (integrated with ACS)
- Up to 874 Inputs system total - each access control panel has 12 inputs and 12 outputs onboard
- Up to 294 Outputs system total - each access control panel has 12 inputs and 12 outputs onboard
- 59 Access Groups
- 19 Schedules
- 2480 Cardholders
- 90 Zones
- 1x Access Control Server
- 3x Access Control Client Workstations

Vendor Responsibility - New Installation; (Supply and Install / Replace)

- Replace 238 Card Readers with HID Multiclass SE Readers (R40)
- Replace 9 Keypad Card Readers with HID Multiclass SE Readers (RK40)
- Replace 17 Access Control Panels to replace ACU hardware
- Replace 113 Single Door Controllers to replace CRC hardware
- Replace 39 Input Boards w/ 16 inputs each board
- Replace 90 Intrusion Keypads to replace KP-DISP hardware
- Install 17 12VDC Power supplies (Altronix AL600ULX or equiv.)
- Replace 17 24VDC Power supplies (Altronix AL600ULX or equiv.)
- Install 1x UPS Rack Mount for Servers (Eaton 9PX1500RT with Eaton 9PXEBM48RT or equiv.)
- Install 1x UPS for workstation SOC only (Eaton 5S1000LCD or equiv.)
- Install any Local Access Control upstream/downstream communication (if required)

2. 340 Laurier Ave, Ottawa, Ontario

Existing;

- 44 Card Readers and associated door hardware
- Up to 284 Inputs system total
- Up to 124 Outputs system
- 59 Access Groups
- 90 Zones
- 1x Access Control Client Workstation

Vendor Responsibility - New Installation; (Supply and Install / Replace)

- Replace 34 Card Readers with HID Multiclass SE Readers (R40)
- Replace 10 Keypad Card Readers with HID Multiclass SE Readers (RK40)

- Replace 4 Access Control Panels to replace ICT hardware
- Replace 5 Input Boards w/ 16 inputs each board
- Replace 4 Intrusion Keypads to replace ICT hardware
- Install 4 12VDC Power supplies (Altronix AL600ULX or equiv.)
- Replace 4 24VDC Power supplies (Altronix AL600ULX or equiv.)
- Install any Local Access Control upstream/downstream communication (if required)

SECTION S – SERVICE AGREEMENT

Overview:
The vendor must provide all ongoing software and integrated solution support services for the Public Safety Canada (PSSP-EISS) in the NCR. The Vendor is to provide

Scope of Work:

1. The Vendor must provide;
   - A single point of contact for ongoing support and maintenance matters.
   - Access to a technical support services via telephone.
   - Provide ongoing support and maintenance of custom integration modules developed for Active Directory integrations.
   - Access to unlimited software updates and upgrades (software only); PS must get access to all latest software releases, upgrades, patches and bug fixes from each subsystem. The Vendor understands that software updates and upgrades must only be implemented upon approval on the production system. PS/SP and the Vendor must work in collaboration to build a schedule for new software qualification and implementation.
   - Provide updates, patches and support to the servers Operating System and all third party applications required in section D.
   - Assistance in building policies and procedures to enable recovery or continuation of PSSP-EISS solution in emergency situations (natural or human induced).

2. One Fulltime support engineer (Monday-Friday 8am-5pm) must be provided to PS/SP as requested, this individual must be responsible for the following activities:

   a. Provide onsite expertise for PSSP-EISS solution as requested and act as a first point of contact for any matter related to PSSP-EISS solution.
   b. Track and manage all service support related tickets raised through PS systems for PSSP-EISS solution, perform root cause analysis of each issue from headquarters as required.
   c. Provide training updates for PS/SP Electronic Security Services employees and security technicians on major content updates, software upgrades and upon addition of new feature set and functionality.
   d. Track and manage warranty status of solution components, initiate and manage warranty requests with each vendor and drive it to closure.

3. The Vendor must provide access to a call centre for service calls on a 24 hours a day, seven days a week basis without relying on third party answering services. To ensure quality responsiveness, the vendor must guarantee a 2-hour response time during normal business hours (Monday-Friday 8am-5pm) and 4-hours response time after hours by a technician in the National Capital Region.

SECTION T – VENDOR DELIVERABLES

1.1 On contract award and before any execution of work, the vendor must provide a detailed approach & methodology proposed to successfully and carefully complete the migration / cut over of the Enterprise Integrated Security System.

1.2 Status reports of activities completed/active/upcoming, schedule & budget variance, issues/risks & proposed responses, and proposed change requests are to occur weekly over contract period.

1.3 All services provided by the Contractor under the Contract must, at the time of acceptance, be free from defects in workmanship and conform with the applicable Codes. If the Contractor must correct or replace the work or any part of the work, it must be at no cost to the Government of Canada.

1.4 All work must be carried out at Public Safety Canada's facilities in Ottawa, ON and must be carried out during regular business hours from Monday-Friday 8am-5pm. It may be required for areas of high level security, between the hours of 18:00 and 06:00 with escorts (48hr notice).

1.5 All communications with Public Safety Canada staff and the Canadian public (*if applicable*) must be performed in the official language (*English or French*) preferred by the employee/citizen.

1.6 All deliverables must be submitted in English.

1.7 PS/SP will arrange for the translation of Contractor-produced deliverables, as required.

1.8 Work shall be performed in accordance with each building management group / PSPC guidelines and applicable local codes or standards current at the commencement of installation. The following list summarizes applicable standards:

i. UL 294 Standard for Access Control Units
ii. UL 294B Standard for Power Over Ethernet (PoE) Power Sources for Access Control Systems and Equipment
iii. UL 302 Standard for the installation, inspection and testing of intrusion alarm systems
iv. ULC 304 Signal Receiving Centre and Premise Burglar Alarm Control Units
v. UL 1076 Standard for Proprietary Burglar Alarm Units and Systems

SECTION U – PS/SP SUPPORT

As required to perform the contract work and at the discretion of the PS/SP Project/Technical Authority, PS/SP will endeavour to provide Contractor personnel with:

i. Relevant internal documentation,
ii. Office space when on site at Public Safety Canada's facilities in Ottawa (*if other arrangements are necessary, they will be made by the PS Project/Technical Authority*),
iii. Scheduled access to the facilities
iv. Provision of timely review, feedback on and approval of deliverables

SECTION V – FUTURE EXPANTION

PS/SP operates in numerous Regional Offices across Canada and the long-term vision is to have those locations integrated on to the new system platform. Although service and installation for

PS regional offices outside Ottawa, ON is not a requirement as part of this phase, the bidder must have the ability to provide installation and services in the cities listed in section Q for future tasks authorisations.

The majority of the project will be completed in Phase 1 (340 Laurier W. et 269 Laurier W.). The amount of employees per regional offices varies between 1 to 30 employees per location, therefore future expansions in regional offices are expected to be minor addition to the system implemented in phase 1.

The exact nature and scope of the work for requirements in regional offices will be determined at a later time when the requirement and location is known.

(End of page)

ACRONYMS and ABBREVIATIONS

AD	Active Directory	SCOM	Microsoft System Center Operations Manager
AES	Advanced Encryption Standard	SCOM	Microsoft System Center Operations Manager
API	Application Programming Interface	NTP	Network Time Protocol
ASIS	ASIS International (American Society for Industrial Security)	NVR	Network Video Recorder
PSSP-EISS	Public Safety / Sécurité publique - Enterprise Integrated Security System		
PS/SP	Public Safety / Sécurité publique Canada	O/S	Operating System
CPP	Certified Protection Professional	PTZ	Pan-Tilt-Zoom
CCTV	Closed Circuit Television	PS	Public Safety Canada
CCTV	Closed Circuit Television System	SPC	Sécurité Publique Canada
CLI	Command Line Interface	PIN	Personal Identification Number
COTS	Commercial-Off-The-Shelf	PSP	Physical Security Professional
CSE	Communications Security Establishment	PoE	Power Over Ethernet
DVMS	Digital Video Management System	QoS	Quality of Service
DVR	Digital Video Recorder	RFID	Radio Frequency Identification
		R	Rated
DVS	Digital Video System	RCMP	Royal Canadian Mounted Police
DNS	Domain Name System	SMTP	Simple Mail Transfer Protocol
DHCP	Dynamic Host Confirmation Protocol	SNMP	Simple Network Management Protocol
EOL	End-of-Line	SSO	Single Sign-On
FTP	File Transfer Protocol	SDK	Software Development Kit
HVAC	Heating, Ventilation and Air Conditioning	SAN	Storage Area Network
HTTP	Hypertext Transfer Protocol	TCP/IP	Transmission Control Protocol/Internet Protocol
IT	Information Technology	TFTP	Trivial File Transfer Protocol
IT/IM	Information Technology/Information Management	UL/ULC	Underwriters Laboratories/Underwriters Laboratories of Canada
ISO	International Standards Organization	UPS	Uninterruptible Power Supply
IP	Internet Protocol	VSAT	Very Small Aperture Terminal
M	Mandatory		
DFSR	Microsoft Distributed File System Replication	VMS	Video Management Software

Name of Firm:

Resource Names:

Signatures:

_____		_____	
Evaluator	Date	Contracting	Date
_____		_____	
Evaluator	Date	Evaluator	Date

SCORING

Met all Mandatories: YES? _____NO? _____

Maximum Score Available: 15

Total Points Achieved: _____

RFP No.:

MANDATORY EVALUATION CRITERIA

Criteria	Criterion	Met/Not Met Comments
M1	The Bidder must propose one **Project Manager.** The bidder is also to propose a team of resources needed and their role in the project that will allow the completion of the required work listed in the Statement of Work. For all proposed resources, the Bidder must submit a detailed resume which clearly describes relevant project descriptions of the resource's work experience. (At least 5 years directly related to security system integration and installations on Enterprise Security Systems) The Bidder should bold-face or highlight the relevant areas in the resource's résumé. At a minimum, the bidder should provide the following information on the résumé: • Full name of the individual proposed; • Education/Academic qualification; • Relevant work experience and the duration of each engagement.	
M2	The Bidder must demonstrate that the proposed team of resources have operated in the security industry, performing security services of similar size and scope to the services described in the Statement of Work (planning, implementation, maintenance, repairs, upgrade to access management, intrusion alarm and installation of an Enterprise Integrated Security System) in the last 10 years. The bidder must identify at a minimum three projects of similar size and scope within the last five years. For each project, the Bidder should provide, at a minimum, the following information:	

RFP No.:

Criteria	Criterion	Met/Not Met Comments
	• Name of client • Description of the project • Identification and role of the resource within the project • Date(s) and duration of project • Rationale for how the project meets the criterion.	
M3	The Bidder must provide **signed** documentation from the bidder's supplier or manufacturer that proves that the bidder is authorized to obtain Technical Support and are able to purchase hardware and software from the supplier or manufacturer. The signed documentation must be on the supplier or manufacturers letter head.	
M4	The bidder MUST demonstrate that the proposed team of resources have successfully **led** a minimum of five (5) projects related to **government access control systems** within the last ten (10) years, where the proposed resources successfully planned, designed, implemented and completed the project. For each project, the Bidder should provide, at a minimum, the following information: • Name of client • Description of the project • Identification and role of the resource(s) within the project • Date(s) and duration of project • Rationale for how the project meets the criterion. One or more of the proposed resources maybe used to satisfy this criterion	

FAILURE OF THE BIDDER TO MEET ALL MANDATORY EVALUATION CRITERIA SHALL RESULT IN A DETERMINATION OF NON-COMPLIANCE AND WILL NOT BE EVALUATED FURTHER

RFP No.:

RATED EVALUATION CRITERIA

Item	Rated Technical Criteria	Maximum points	Demonstrated Compliance
	Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below. **The Bidder must provide sufficient detail to clearly demonstrate how they meet each rated requirement below. Bidders are advised that only listing experience without providing any supporting data and information to describe responsibilities, duties and relevance to the requirements, or reusing the same wording as the RFP, will not be considered "demonstrated" for the purpose of this evaluation.**		

R1 –The Bidder's proposed **Project Manager** will be evaluated on a point rated basis with respect to their years of experience in installation of Access Control Systems of similar size, scale and complexity.

5 points will be awarded for each additional year of project experience of similar size and scope (after 5 years of mandatory experience identified at M1). (Max. of 15 points)

Total maximum R1 technical points	**15 points**
Total R1 points received	

COMMON-PS-SRCL#2

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
Security Classification / Classification de sécurité UNCLASSIFIED	

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Public Safety Canada	Corporate Management Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Public Safety / Sécurité publique Canada (PSSP) National Headquarters in the National Capital Region currently has a requirement to upgrade their legacy Access Control/ Intrusion System. The current legacy systems are based on 1. Summit Enterprise eNT and 2. ICT Protégé System. The requirement is to upgrade to a centralized modern Enterprise Integrated Security System with which to protect, defend and respond to actual and potential security and life-safety events and situations affecting its people, assets and information.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☑ No / Non	☐ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☐ No / Non	☑ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☐	NATO / OTAN ☐	Foreign / Étranger ☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions Aucune restriction relative à la diffusion ☐	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A PROTÉGÉ A ☐	NATO UNCLASSIFIED NATO NON CLASSIFIÉ ☐	PROTECTED A PROTÉGÉ A ☐
PROTECTED B PROTÉGÉ B ☐	NATO RESTRICTED NATO DIFFUSION RESTREINTE ☐	PROTECTED B PROTÉGÉ B ☐
PROTECTED C PROTÉGÉ C ☐	NATO CONFIDENTIAL NATO CONFIDENTIEL ☐	PROTECTED C PROTÉGÉ C ☐
CONFIDENTIAL CONFIDENTIEL ☐	NATO SECRET NATO SECRET ☐	CONFIDENTIAL CONFIDENTIEL ☐
SECRET SECRET ☐	COSMIC TOP SECRET COSMIC TRÈS SECRET ☐	SECRET SECRET ☐
TOP SECRET TRÈS SECRET ☐		TOP SECRET TRÈS SECRET ☐
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité UNCLASSIFIED

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
Security Classification / Classification de sécurité UNCLASSIFIED	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Eric Poulin	Manager, Security Operations		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 991-5838		eric.poulin@canada.ca	25/11/2019

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Jean-Francois Houde	Manager, Security Services		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 949-6420			NOV 25 2019

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

☒ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
		Saumur, Jacques 0 Digitally signed by Saumur, Jacques 0 DN: c=CA, o=GC, ou=PWGSC-TPSGC, cn=Saumur, Jacques 0 Date: 2017.02.02 11:38:22 -05'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**

Jacques Saumur
Contract Security Officer
Contracts Security Division|Division des contrats sécurité /
Contract Security Program|Programme de sécurité des contrats /
Public Services and Procurement Canada| Services publics et Approvisionnement Canada
Jacques.Saumur@tpsgc-pwgsc.gc.ca
Telephone | Téléphone 613-948-1732
Facsimile | Télécopieur 613-948-1712

ANNEX G NON-DISCLOSURE AGREEMENT

I, _____ , recognize that in the course of my work as an employee or subcontractor of _____ , I may be given access to information by or on behalf of Canada in connection with the Work, pursuant to Solicitation and Contract Serial No. 0D160-204228 between Her Majesty the Queen in right of Canada, represented by the Minister of Public Works and Government Services and Public Safety Canada (PS) , including any information that is confidential or proprietary to third parties, and information conceived, developed or produced by the Contractor as part of the Work. For the purposes of this agreement, information includes but not limited to: any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form, recorded electronically, or otherwise and whether or not labeled as proprietary or sensitive, that is disclosed to a person or that a person becomes aware of during the performance of the Contract.

I agree that I will not reproduce, copy, use, divulge, release or disclose, in whole or in part, in whatever way or form any information described above to any person other than a person employed by Canada on a need to know basis. I undertake to safeguard the same and take all necessary and appropriate measures, including those set out in any written or oral instructions issued by Canada, to prevent the disclosure of or access to such information in contravention of this agreement.

I also acknowledge that any information provided to the Contractor by or on behalf of Canada must be used solely for the purpose of the Contract and must remain the property of Canada or a third party, as the case may be.

I agree that the obligation of this agreement will survive the completion of the Contract Serial No.: 0D160-204228/001/HN

_____
Name (print)

_____
Signature

_____
Tittle

_____
Date

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

Claim for Exchange Rate Adjustments
Demande de rajustement du taux de change

Contractor Name - Nom de l'entrepreneur	PWGSC File Number - Numéro du dossier de TPSGC	Contract Number - Numéro du contrat	Item/Invoice Number - Numéro d'article/de facture

1	2	3	4	5	6	7	8	9
Item Number Numéro d'article	Description	Foreign Currency Component (FCC) per Unit Montant en monnaie étrangère par unité **($CAN)**	Foreign Currency Devise étrangères	Quantity Quantité	Initial Exchange Rate Facteur de conversion initial **(i_0)**	Exchange Rate for Adjustments Taux de change aux fins du rajustement **(i_1)**	% Change Variation en % **$(i_1-i_0)/i_0 > 0.02$ (+/-)**	Adjustment = FCC X Quantity X **$(i_1 - i_0)/i_0$** Rajustement = montant en monnaie étrangère X Quantité X **$(i_1 - i_0)/i_0$**
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
					Total Exchange Rate Adjustment Rajustement total du taux de change			**$ 0.000**

Instructions

Where:

i_0 = initial exchange rate (CAN$ per unit of foreign currency [e.g. US$1])

i_1 = exchange rate for adjustment purposes (CAN$ per unit of foreign currency [e.g. US$1])

Instructions to bidders:

1. Bidders must complete columns (1) to (4) at time of bidding, for each line item where they want to invoke the exchange rate fluctuation provisions.

2. Where bids are evaluated in Canadian dollars, the dollar values provided in column (3) should also be in Canadian dollars, so that the adjustment amount is in the same currency as the payment.

Instructions for Payment:

1. This form must be submitted with the invoice for payment with respect to all items with an FCC. Complete columns (1) through (7). Columns (8) and (9) will auto complete.

2. Suppliers should submit a separate calculation sheet for each invoice submitted showing the exchange rate adjustment for all line items with an FCC.

3. This form must be provided with all invoices where the exchange rate fluctuates more than 2% (increase or decrease), (i.e. $abs[(i_1 - i_0) / i_0] > .02$), unless otherwise stated in the contract.

Étant entendu que :

i_0 = Facteur de conversion du taux de change initial ($ CA par unité de devise étrangère [p. ex. 1 $ US])

i_1 = Taux de change aux fins du rajustement ($ CA par unité de devise étrangère [p. ex. 1 $ US])

Instructions aux soumissionnaires :

1. Les soumissionnaires doivent remplir les colonnes (1) à (4) au moment de présenter leur soumission, pour chacun des produits pour lesquels ils veulent se prévaloir des dispositions relatives à la fluctuation du taux de change.

2. Lorsque les soumissions sont évaluées en dollars canadiens, les montants en dollars indiqués dans la colonne (3) doivent également être en dollars canadiens, de sorte que le montant du rajustement soit indiqué dans la même devise que pour le paiement.

Instructions relatives au paiement :

1. Le présent formulaire doit accompagner la facture en vue du paiement pour chaque article comportant un montant en monnaie étrangère. Il faut remplir les colonnes (1) à (7). Les colonnes (8) et (9) seront remplies automatiquement.

2. Les fournisseurs doivent présenter une feuille de calcul séparée pour chaque facture et indiquer le rajustement du taux de change pour chaque article comportant un montant en monnaie étrangère.

3. Le présent formulaire doit accompagner toutes les factures pour lesquelles la fluctuation du taux de change est supérieure à 2% (augmentation ou diminution), (c.-à-d. $abs[(i_1 - i_0) /i_0] > .02$), à moins d'indication contraire dans le contrat.