PARLIAMENTARY PROTECTIVE SERVICE
SERVICE DE PROTECTION PARLEMENTAIRE

CANADA

Request for Proposal

For

Computer Aided Dispatch System

Request for Proposal No: PPS-RFP-2020-060
Date of Issue: August 17, 2020
Submission Deadline: September 28, 2020

CONTINUATION

TABLE OF CONTENTS

CONTINUATION

PART 1 – INTRODUCTION

1.1   Invitation to Bidders

This Request for Proposals ("the RFP") issued by the Parliamentary Protective Service (PPS) is an invitation to submit non-binding offers for the provision of a **Computer Aided Dispatch (CAD) system** as further described in Appendix D, for the prices established in Appendix C. The Bidder(s) selected pursuant to this RFP process will be informed in writing. Bidders not selected will also be informed in writing.

Consortium or Joint Venture Proposals

Responses submitted by a Bidder that consists of more than one legal entity or person (such as consortia or joint ventures) will be accepted with the understanding that PPS shall regard only one of the parties of the consortium or joint venture as the prime Supplier. Responses shall clearly indicate which party is the prime Supplier. The prime Supplier shall be solely accountable for all additional parties. PPS will enter into an agreement only with the prime supplier.

1.2   Type of Agreement for Deliverables

It is the Parliamentary Protective Service's intention to enter into an agreement with one legal entity. The term of the agreement is to be for a period of three (3) years, with options in favour of the Parliamentary Protective Service to extend the agreement on the same terms and conditions for up to two (2) one-year (1) periods.

1.3   No guarantee of Volume of Work or Exclusivity of Agreement

The Parliamentary Protective Service makes no guarantee of the value or volume of work to be assigned to the successful Bidder. The agreement to be negotiated with the selected Bidder will not be an exclusive agreement for the provision of the described deliverables. The Parliamentary Protective Service may put in place an agreement with others for the same or similar deliverables to those described in the RFP or may obtain the same or similar deliverables internally.

1.4   Submission Instructions

1.4.1   Bidders must submit their response in accordance with the following timetable and instructions.

Issue Date of RFP	**August 17, 2020**
Deadline for Questions	**September 14, 2020 at 14:00 EST**
Submission Deadline	**September 28, 2020 at 14:00 EST**

The above timetable is a tentative schedule and may be amended by the Parliamentary Protective Service at any time.

Bidders must submit their Submission Form (Appendix B) in the form prescribed herein by the Submission Deadline to the Parliamentary Protective Service Contact identified below in the manner set out below:

1.4.2   Parliamentary Protective Service Contact:
Wayne Dubeau
Senior Contracting Officer
E-mail: Proposals-soumissions@pps-spp.parl.gc.ca

CONTINUATION

PART 1 – INTRODUCTION

1.4.3   Responses must be submitted electronically to the email address listed above. No hard copies will be accepted.

1.4.4   Bidders are solely responsible for the delivery of their responses in the manner and time prescribed. Responses received after the Submission Deadline will be rejected.

1.4.5   All responses must include the following mandatory forms:

      1.4.5.1 Proposal Submission Form (Appendix B), completed in its entirety and signed by an authorized representative of the Bidder;

      1.4.5.2 Pricing Structure Form (Appendix C), completed in accordance with the instructions contained within Appendix C, Pricing Structure Form.

      1.4.5.3 Other than inserting the information requested on these mandatory forms, a Bidder may not make any changes to any of the forms.

1.5   Communications During Solicitation Period

1.5.1   Unless otherwise specified, all enquiries concerning this RFP must be received by email no later than 14:00:00 (EST) on September 14, 2020 to the following PPS contact:

Wayne Dubeau
Senior Contracting Officer
Procurement and Contracting Services
155 Queen Street, 5th Floor
Ottawa ON K1A 0B8
Email: Proposals-soumissions@pps-spp.parl.gc.ca

1.5.2   All questions submitted by Bidders by email to the PPS Contracting Authority will be deemed to be received once the email has entered the PPS' email inbox. No such communications are to be directed to anyone other than the PPS Contracting Authority at the address above in clause 1.5.1. Questions received after the closing time may not be answered.

1.5.3   PPS is under no obligation to provide additional information, and PPS will not be responsible for any information provided by or obtained from any source other than the PPS Contracting Authority.

1.5.4   It is the responsibility of the Bidder to seek clarification from the PPS Contracting Authority prior to the time set out in clause 1.5.1 on any matter it considers to be unclear. PPS will not be responsible for any misunderstanding on the part of the Bidder concerning the RFP or the procurement process.

CONTINUATION

PART 1 – INTRODUCTION

1.6 <u>**Amendment and Withdrawl of Responses**</u>

1.6.1 Bidders may amend their responses prior to the closing date of the RFP by submitting the amendment electronically to the PPS email address listed in 1.4.2. The amendment must contain the RFP title and number and the full legal name of the Bidder. Any such amendment should clearly indicate which part of the response the amendment is intended to replace.

1.6.2 At any time throughout the RFP process, a Bidder may withdraw a submitted response. To affect a withdrawal, a notice of withdrawal must be sent to the Parliamentary Protective Service Contact and must be signed by an authorized representative. The Parliamentary Protective Service is under no obligation to return withdrawn responses.

CONTINUATION

PART 2 – EVALUATION OF PROPOSALS

2.1 EVALUATION OF RESPONSES

2.1.1 An Evaluation Team has been assembled to review the responses, assess their compliance against the selection and evaluation criteria of this RFP, and consider accepting the responses of one or more compliant Bidders. The criteria to be used by the Evaluation Team to assess and rate the responses are shown in Appendix E, Evaluation Criteria and Financial Evaluation. All aspects of the criteria should be thoroughly addressed by Bidders. Those Bidders responding with unqualified phrases such as "we comply", will not be rated as highly as those Bidders that described in some detail just how they comply.

2.1.2 While price is a factor in the selection of the successful Bidder(s), other criteria are weighted and will be evaluated accordingly. PPS reserves the right not to invite any top-ranked Bidder(s) to enter negotiations where:

Following the Financial Evaluation, a Bidder's Total Evaluated Score is ranked among the top-ranked Bidders (as determined on the basis of stage III to be invited) on the strength of their Financial Proposal, such that their evaluated Technical Evaluation is more than twenty percent (20%) below the threshold established by the last of the ranked Bidders.

In such cases, and at its sole discretion, PPS may seek pricing clarification from the Bidder, or proceed to the next highest technically competent Bidder.

2.2 STAGES OF EVALUATION

The Parliamentary Protective Service will conduct the evaluation of all proposals received in the manner and time provided in accordance with the following four (4) stages:

2.2.1 Stage I – Solution Criteria, Submission and Rectification

2.2.1.1 Stage I will consist of a review to determine which proposals are complete and provide all required information to perform the subsequent stages of evaluation. Bidders whose proposals are incomplete as of the Submission Deadline will be provided an opportunity to rectify any deficiencies related to completeness within the Rectification Period. Proposals failing to be deemed complete within the Rectification Period will be excluded from further consideration. The Rectification Period will begin to run from the date and time that the Parliamentary Protective Service notifies a Bidder in writing.

2.2.1.2 Proposal Submission Form
Proposals must include a Proposal Submission Form (Appendix B) completed in its entirety and signed by an authorized representative of the Bidder.

2.2.1.3 Pricing Structure Form
Proposals must include a Pricing Structure Form (Appendix C).
(a)   prices must be provided in Canadian funds, inclusive of all applicable duties and taxes which should be itemized separately; and

CONTINUATION

PART 2 – EVALUATION OF PROPOSALS

prices quoted by the Bidder must be all-inclusive and must include all labour and material costs, all travel and carriage costs, all insurance costs, all costs of delivery to the Parliamentary Protective Service, all costs of installation and set-up, including any pre-delivery inspection charges, and all other overhead, including any fees or other charges required by law.

2.2.2   Stage II – Evaluation of the Rated Criteria

Stage II will consist of a scoring by the Parliamentary Protective Service of each complete proposal based on the rated criteria as described in Appendix E.

2.2.3   Stage III – Evaluation of Pricing

2.2.3.1 <u>Evaluation of Price</u>

Stage III will consist of a scoring of the pricing submitted. The evaluation of pricing will be undertaken after the evaluation of the rated criteria has been completed. Only those Bidders whose proposals meet the mandatory minimum threshold scores for Rated Criteria (Stage II) will have their Financial Proposal evaluated.

2.2.3.2 <u>Cumulative Score and Selection of Highest Scoring Bidders</u>

At the conclusion of Stage III, Bidders' scores from Stage II and Stage III will be added together and up to the threehighest-ranked Bidders will be selected for Stage IV.

2.2.4   Stage IV – Functional Demonstration

Up to the three highest-ranked Bidders may be invited to participate in a demonstration to exhibit how their proposed computer aided dispatch system meets the functional and technical requirements set out in the RFP. Scenarios may be constructed and provided to the bidders in advance. Bidders will be ranked on a point system and their scores will be added to the technical and financial scores in order to establish a ranked order. Based on this ranking, the PPS will begin negotiations with the top-ranked bidder.

If any of the highest-ranked Bidders fail the functional demonstration, the Parliamentary Protective Service may choose to invite the next highest ranked Bidder(s) to participate in a demonstration.

PPS reserves the right to invite additional Bidders whose evaluated score is within 10% of the lowest highest-ranked Bidder as determined by the evaluation of stage II.

2.3   <u>Rated Criteria</u>

In addition to submitting the Proposal Submission Form, noted above, Bidders should respond to the non-price factors described in Appendix E.

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

3.1 **BIDDERS TO FOLLOW INSTRUCTIONS**

Bidders should structure their responses in accordance with the instructions in the RFP. Where information is requested in the RFP, any response made in a proposal should reference the applicable clause numbers of the RFP where that request was made.

In the event of any discrepancies between the English and French versions of this RFP, the English version of the RFP document will prevail.

In the event of any discrepancies between the notice posted on Buy and Sell and this RFP document, the information in this RFP document will prevail.

3.2 **COMMUNICATION OF RFP DOCUMENTS AND ADDENDA**

The Parliamentary Protective Service will only post RFP documents and any associated Addenda via email.

3.3 **INFORMATION IN RFP AN ESTIMATE ONLY**

The Parliamentary Protective Service makes no representation, warranty or guarantee as to the accuracy of the information contained in this RFP or issued by way of addenda. Any quantities shown or data contained in the RFP or provided by way of addenda are estimates only and are for the sole purpose of indicating to Bidders the general size of the opportunity. It is the Bidder's responsibility to avail itself of all the necessary information to prepare a proposal in response to the RFP.

3.4 **BIDDERS SHALL BEAR THEIR OWN COSTS**

Each Bidder shall bear all costs associated with or incurred in the preparation and presentation of its response, including, if applicable, costs incurred for acceptance testing or presentations.

3.5 **COMMUNICATION AFTER ISSUANCE OF RFP**

3.5.1 **Bidders to Review RFP**

3.5.1.1 Bidders should promptly examine all of the documents comprising the RFP, and

(a) report any errors, omissions or ambiguities; and

(b) direct questions or seek additional information by email to the Parliamentary Protective Service Contact as set out in Part 1, clause 1.4.2.

3.5.1.2 The Parliamentary Protective Service is under no obligation to provide additional information, and the Parliamentary Protective Service is not responsible for any information provided by or obtained from any source other than the Parliamentary Protective Service Contact.

3.5.1.3 It is the responsibility of the Bidder to seek clarification from the Parliamentary Protective Service Contact on any matter it considers to be unclear. The Parliamentary Protective Service is not responsible for any misunderstanding on the part of the Bidder concerning the RFP or the procurement process.

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

3.5.2 All New Information to Bidders by Way of Addenda

3.5.2.1 The RFP may be amended only by an addendum in accordance with this clause. If the Parliamentary Protective Service, for any reason, determines that it is necessary to provide additional information relating to the RFP, such information will be communicated to all Bidders by addenda. Each addendum forms an integral part of the RFP.

3.5.2.2 Such addenda may contain important information, including significant changes to the RFP. Bidders are responsible for obtaining all addenda issued by the Parliamentary Protective Service. In the Proposal Submission Form (Appendix B), Bidders should confirm their receipt of all addenda by setting out the number of each addendum in the space provided.

3.5.3 Post-Deadline Addenda and Extension of Submission Deadline

If any addendum is issued after the Deadline for Issuing Addenda (if applicable), the Parliamentary Protective Service may at its discretion extend the Submission Deadline for a reasonable amount of time.

3.5.4 Verify, Clarify & Supplement

When evaluating responses, the Parliamentary Protective Service may request further information from the Bidder or third parties in order to verify, clarify or supplement the information provided in the Bidder's response. The Parliamentary Protective Service may revisit and re-evaluate the Bidder's response or ranking based on any such information.

3.5.5 No Incorporation by Reference

The entire content of the Bidder's response should be submitted in a fixed form (PDF format).

The content of websites or other external documents referred to in the Bidder's response will not be considered to form part of its response. Bidders should include any reference material they wish to be considered for evaluation within their response. Any material or documents outside the response will not be considered. Should a Bidder wish to provide screen shots of its website for evaluation, copies or printouts of website material should be included within the response. URL links to the Bidder's website will not be considered by the Parliamentary Protective Service Evaluation Team.

3.5.6 Responses to be retained by the Parliamentary Protective Service

The Parliamentary Protective Service will not return the response, or any accompanying documentation submitted by a Bidder.

3.6 NEGOTIATIONS, NOTIFICATION AND DEBRIEFING

3.6.1 Selection of Highest-Ranked Bidder(s)
The highest-ranked Bidder(s), as established under Part 2, Evaluation of Responses, will receive a written invitation to enter negotiations with the Parliamentary Protective Service.

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

3.6.2 Timeframe for Negotiations

The Parliamentary Protective Service intends to conclude negotiations with the highest-ranked Bidder within ten (10) business days commencing from the date the Parliamentary Protective Service invites the highest-ranked Bidder to enter negotiations. A Bidder invited to enter negotiations should therefore be prepared to provide requested information in a timely fashion and to conduct its negotiations expeditiously.

3.6.3 Process Rules for Negotiation

Any negotiations will be subject to the process rules contained in this Part 3, Terms and Conditions of the Procurement Process and Appendix B, Proposal Submission Form and will not constitute a legally binding offer to enter into an agreement on the part of the Parliamentary Protective Service or the Bidder. Negotiations may include requests by the Parliamentary Protective Service for supplementary information from the Bidder to verify, clarify or supplement the information provided in its response or to confirm the conclusions reached in the evaluation, and may include requests by the Parliamentary Protective Service for improved pricing from the Bidder.

3.6.4 Terms and Conditions

The terms and conditions that will form any resulting agreement will be provided to the highest-ranked Bidder prior the commencement of the negotiation process and will form the starting point for negotiation.

3.6.5 Failure to Enter into Agreement

Bidders should note that if the parties cannot execute an agreement within the allotted ten (10) business days, the Parliamentary Protective Service may invite the next highest-ranked Bidder to enter negotiations. In accordance with the process rules in this Part 3, Terms and Conditions of the Procurement Process and clause 2 of Appendix B, the Proposal Submission Form, there will be no legally binding relationship created with any Bidder prior to the execution of a written agreement. With a view to expediting agreement formalization, at the midway point of the above-noted timeframe, the Parliamentary Protective Service may elect to initiate concurrent negotiations with the next-highest-ranked Bidder. Once the above-noted timeframe lapses, the Parliamentary Protective Service may discontinue further negotiations with the highest-ranked Bidder. This process will continue until an agreement is formalized, until there are no more Bidders remaining that are eligible for negotiations or until the Parliamentary Protective Service elects to cancel the procurement process.

3.6.6 Notification to Other Bidders

Other Bidders that become eligible for negotiations will be notified at the commencement of their respective negotiations. Once an agreement is executed between the Parliamentary Protective Service and a Bidder, the other Bidders may be notified directly in writing and/or will be notified by public posting in the same manner that the RFP was originally posted of the outcome of the procurement process and the award of the agreement.

3.6.7 Debriefing

Bidders may request a debriefing after receipt of a notification of award. All requests must be in writing to the Parliamentary Protective Service Contact and must be made within thirty (30) calendar days of notification of award. The intent of the debriefing information session is to aid the Bidder in

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

presenting a better response in subsequent procurement opportunities. Any debriefing provided is not for the purpose of providing an opportunity to challenge the procurement process.

3.7 CONFLICT OF INTEREST AND PROHIBITED CONDUCT

3.7.1 Conflict of Interest
The Parliamentary Protective Service may disqualify a Bidder for any conduct, situation or circumstances, as solely determined by the Parliamentary Protective Service, that constitutes a Conflict of Interest. For the purposes of this clause, "Conflict of Interest" will have the meaning ascribed to it in clause 7 of the Proposal Submission Form (Appendix B).

3.7.2 Prohibited Bidder Communications
Bidders will not engage in any communications as described in clause 7.1.2 of the Proposal Submission Form (Appendix B). Bidders should also take note of the Conflict of Interest declaration set out in the Proposal Submission Form (Appendix B).

3.7.3 Bidder Not to Communicate with Media
Bidders may not at any time directly or indirectly communicate with the media in relation to the RFP or any agreement awarded pursuant to the RFP without first obtaining the written permission of the Parliamentary Protective Service Contact.

3.7.4 No Lobbying
Bidders may not in relation to the RFP or the evaluation and selection process in respect thereof, engage in any form of political or other lobbying whatsoever to influence the selection of the approved Bidder(s). Further, no Bidder or any person affiliated to a Bidder will attempt to communicate in relation to the RFP or a Bidder's response, directly or indirectly, with any director, officer, employee or other representative of the Parliamentary Protective Service, except as expressly directed or permitted by the RFP.

3.7.5 Illegal or Unethical Conduct
Bidders will not engage in any illegal bidding practices, including such activities as bid-rigging, price-fixing, bribery, fraud or collusion. Bidders will not engage in any unethical conduct, including lobbying or other inappropriate communications, offers of gifts to Parliamentary Protective Service employees, deceitfulness, submitting responses containing misrepresentations or other misleading or inaccurate information, or any other conduct that compromises or may be seen to compromise the procurement process.

3.7.6 Past Performance or Inappropriate Conduct
The Parliamentary Protective Service may prohibit a supplier from participating in a procurement process based on past performance or based on inappropriate conduct in a prior procurement process, and such inappropriate conduct includes but is not be limited to the following: (a) the submission of quotations containing misrepresentations or any other inaccurate, misleading or incomplete information; (b) the refusal of a supplier to honour its pricing or other commitments made in a response or bid; or (c) any other conduct, situation or circumstance, as solely determined by the Parliamentary Protective Service, that constitutes a Conflict of Interest. For the purposes of this clause, "Conflict of Interest" will have the meaning ascribed to it in the Proposal Submission Form (Appendix B).

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

3.8 **CONFIDENTIAL INFORMATION**

3.8.1 All information provided by or obtained from the Parliamentary Protective Service in any form in connection with the RFP either before or after the issuance of the RFP

3.8.1.1 is the sole property of the Parliamentary Protective Service and must be treated as confidential;

3.8.1.2 is not to be used for any purpose other than replying to the RFP and the execution of any subsequent agreement;

3.8.1.3 must not be disclosed without prior written authorization from the Parliamentary Protective Service; and

3.8.1.4 will be returned by the Bidders to the Parliamentary Protective Service immediately upon the request of the Parliamentary Protective Service.

3.8.2 Confidential Information of Bidder
Bidders should identify any information in their response or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by the Parliamentary Protective Service. The confidentiality of such information will be maintained by the Parliamentary Protective Service, except as otherwise required by law or by order of a court or tribunal. Bidders are advised that their responses will, as necessary, be disclosed on a confidential basis, to the Parliamentary Protective Service's advisors retained for the purpose of evaluating or participating in the evaluation of their responses. If a Bidder has any questions about the collection and use of information pursuant to the RFP, questions are to be submitted to the Parliamentary Protective Service Contact.

3.9 **PROCUREMENT PROCESS NON-BINDING**

3.9.1 No Contract A and No Claims
The procurement process is not intended to create and does not create a Contract A bidding process nor any contractual or other legally enforceable obligations. The procurement process is instead governed by the law applicable to direct commercial negotiations. For greater certainty and without limitation:

3.9.1.1 Neither the Bidder nor the Parliamentary Protective Service has the right to make any claims (in contract, tort, or otherwise) against the other with respect to the award of an agreement, failure to award an agreement or failure to honour a response to the RFP.

3.9.2 No agreement until execution of written agreement
The procurement process is intended to identify prospective suppliers for the purposes of negotiating potential agreements. No legal relationship or obligation regarding the procurement of any good or service will be created between a Bidder and the Parliamentary Protective Service by the procurement process. An agreement will only exist following successful negotiation and execution of a written agreement for the acquisition of goods and/or services.

CONTINUATION

PART 3 – TERMS AND CONDITIONS OF THE PROCUREMENT PROCESS

3.9.3 Non-binding price estimates
While the pricing information provided with responses will be non-binding prior to the execution of a written agreement, such information will be assessed during the evaluation of responses and the ranking of the Bidders. Any inaccurate, misleading or incomplete information, including withdrawn or altered pricing, could have an adverse impact on any such evaluation, ranking or agreement award.

3.9.4 Disqualification for Misrepresentation
The Parliamentary Protective Service may disqualify the Bidder or rescind an agreement subsequently entered into if the Bidder's response contains misrepresentations or any inaccurate, misleading or incomplete information.

3.9.5 References and Past Performance
The Parliamentary Protective Service's evaluation may include information provided by the Bidder's references and may also consider the Bidder's past performance on previous agreements with the Parliamentary Protective Service.

3.9.6 Cancellation
The Parliamentary Protective Service may cancel or amend this procurement process without liability at any time.

3.10 GOVERNING LAW AND INTERPRETATION

3.10.1 Governing Law
The terms and conditions in this Part 3, Terms and Conditions of the Procurement Process are:

3.10.1.1 included for greater certainty and are intended to be interpreted broadly and separately (with no particular provision intended to limit the scope of any other provision);

3.10.1.2 non-exhaustive (and will not be construed as intending to limit the pre-existing rights of the parties to engage in pre-contractual discussions in accordance with the common law governing direct commercial negotiations); and

3.10.1.3 to be governed by and construed in accordance with the laws of the province of Ontario and the federal laws of Canada applicable therein.

3.10.2 Language Interpretation
In the event of any discrepancies between the English and French versions of this solicitation document, the language of the English version will be interpreted as correct.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

1. **GOVERNING LAWS AND JURISDICTION**

The agreement shall, for all purposes, be governed by and construed in accordance with the laws of the Province of Ontario. The Supplier irrevocably attorns to the exclusive jurisdiction of the courts of Ontario with respect to any matter arising under or related to this agreement and related purchase orders.

2. **PRIORITY OF DOCUMENTS**

The documents specified below form part of and are incorporated into the agreement. If there is a discrepancy between the wordings of any documents that appear on the list, the wording of the document that first appears shall prevail over the wording of any document that subsequently appears on the list.

2.1. Appendix A, Framework Agreement Terms and Conditions;
2.2. Appendix B, Proposal Submission Form;
2.3. Appendix C, Pricing Structure;
2.4. Appendix D, Statement of Requirements.

3. **TIME IS OF THE ESSENCE**

The work must be performed within or at the time stated in the agreement.

4. **REQUIREMENT**

The Supplier shall use the methodology described in its proposal, provide the services and goods required to meet the requirements set out in Appendix D, as specified in this agreement.

5. **STATUS OF CAPACITY**

The Supplier has represented and does hereby warrant that:

5.1 it has the personnel, experience, qualifications, equipment, facilities and all other skills and resources necessary to provide the goods and/or services to the Parliamentary Protective Service required herein and to do so in an efficient and timely manner, and

5.2 all goods and/or services provided under this agreement shall meet or exceed industry standards and shall be provided in accordance with applicable law.

6. **PERIOD OF AGREEMENT**

6.1 The Supplier will perform the tasks and provide the services outlined herein and any attached Schedules and/or Appendices, from the date of award for a period of three (3) years, in accordance with the Terms and Conditions listed herein.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

6.2   The Parliamentary Protective Service reserves the irrevocable option of extending this agreement under the same terms and conditions for an additional two (2) one (1) year periods.

6.3   The last day of the term or any extension of the term of this agreement indicated on page one (1) shall be known as the expiry date. This is the last day that an order may be issued pursuant to this agreement. All such orders are to be honoured, notwithstanding that delivery will occur after the expiry date. Delivery must be completed within thirty (30) days after the expiry date of this agreement. No order is to be issued pursuant to this agreement after the expiry date.

7.   LIMITATION OF EXPENDITURE

No increase in the total liability of the Parliamentary Protective Service with regard to the price of the goods and services resulting from any design changes, modifications or interpretation of specifications, will be authorized or paid to the Supplier, unless such design changes, modifications or interpretations of specifications have been approved by the Parliamentary Protective Service' Contracting Authority in writing prior to their incorporation in the work.

8.   TRAVEL EXPENSE PROVISION

The cost of the travel, accommodation and meals incurred by the Supplier are for the Supplier's account and will not be paid by the Parliamentary Protective Service.

9.   GOODS AND SERVICES TAX (GST) / HARMONIZED SALES TAX (HST)

The GST or any other federal tax such as the HST is not included in the firm price. This tax, to the extent applicable, is to be shown separately on all invoices and will be paid by the Parliamentary Protective Service. The Supplier's federal tax registration number must appear on invoices when that federal tax is being charged. The Supplier agrees to bill and collect any applicable federal tax and to remit to the Canada Revenue Agency any federal tax received from the Parliamentary Protective Service.

10.   PROVINCIAL SALES TAX (PST) IN PROVINCES OTHER THAN QUEBEC

10.1   The Parliamentary Protective Service is PST exempt, but is subject to GST and HST as indicated in clause 9.

10.2   If a PST license number or a signed certificate of exemption is required, it will be provided upon request. The Parliamentary Protective Service recognizes the requirements set out in the legislation of the provinces where PST applies and, as such, all purchasing orders, purchase documents, acquisition card forms and agreements issued by the Parliamentary Protective Service will make reference to the appropriate PST licence number.

11.   QUEBEC SALES TAX (QST)

11.1   The Parliamentary Protective Service will pay the QST, if applicable.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

11.2   The QST is not included in the firm price. This tax, to the extent applicable, is to be shown separately on all invoices. The Supplier agrees to invoice and collect from the Parliamentary Protective Service the QST and to further remit it to Revenue Quebec as required. The Supplier's QST registration number must appear on invoices when that tax is being charged.

12.   PROVINCIAL ANCILLARY TAXES AND REGULATORY CHARGES

12.1   For the purpose of this clause, an ancillary tax is a tax levied pursuant to a provincial statute other than the provincial retail sales tax legislation or its equivalent and the primary aspect of which is to raise revenue, whereas a regulatory charge is a charge introduced in a provincial legislative instrument other than in retail sales tax legislation or its equivalent and whose primary purpose is to finance a regulatory scheme.

12.2   The Parliamentary Protective Service is exempt from paying any ancillary taxes, but agrees to pay any applicable regulatory charge. In the event that a regulatory charge applies, it will not be included in the firm price.

13.   PRICING

For the successful provision of the goods and services detailed herein, the Supplier shall be paid according to the pricing schedule of this agreement. The prices are excluded of any PST, QST, GST and HST taxes and should include all applicable Canadian customs and excise taxes, and are FOB Destination.

14.   METHOD OF PAYMENT

14.1   Subject to the approval of the appropriate authority of the Parliamentary Protective Service, payment by the Parliamentary Protective Service for goods and/or services will be made within thirty (30) days following the date on which goods and/or services have been received in accordance with the terms and conditions of the agreement or within thirty (30) days following the date on which an invoice has been received by the Parliamentary Protective Service' Financial Management Operations, along with the substantiating documentation, whichever date is the later.

14.2   Final payment will not be made until all deliverables have been submitted and judged satisfactory by the Parliamentary Protective Service' Project Authority.

14.3   All invoices must indicate the above agreement number and any applicable PO number and are to be submitted by email to finance-finances@pps-spp.parl.gc.ca and/or to the PPS Project Authority named in Section 31.

15.   CANCELLATION OF AGREEMENT

15.1   The agreement may be terminated at any time and for any reason by the Parliamentary Protective Service with a ten (10) working days written notice.

15.2   The agreement may be terminated in writing at the discretion of the Parliamentary Protective Service, without prior notice, if the Supplier is for any reason unable to provide the goods or services required under the agreement.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

15.3 The agreement may be terminated at the discretion of the Parliamentary Protective Service if, during the term of the agreement all or any part of the property, goods or effects of the Supplier are at any time seized or taken in execution or by attachment or if the Supplier makes an unauthorized assignment or becomes bankrupt or insolvent.

15.4 Upon the termination of the agreement prior to the expiry date, the Supplier shall be entitled to be paid an amount that, by mutual agreement of both parties, is equal to the work performed by the Supplier for the Parliamentary Protective Service to the date of termination, less any amounts that have previously been paid to the Supplier.

15.5 In the event of termination, the Supplier must forthwith give to the Parliamentary Protective Service all completed work and work-in-progress, including all software, data, programs, systems documentation, research, reports, papers, materials and other information relating to the completed work and work-in-progress.

16. AMENDMENTS TO AGREEMENT

No modification to the agreement shall be valid unless it is in writing and signed by each party hereto. All proposed changes to the agreement must be submitted to the Parliamentary Protective Service' Contracting Authority identified in clause 31.

17. CONFIDENTIALITY

17.1 All information relating to the affairs of the Parliamentary Protective Service or of its employees, or of Members or their employees, to which the Supplier, or any officer or servant of the Supplier, becomes privy as a result of the work to be done under the agreement must be treated as confidential during and after the performance of the services.

17.2 Upon expiry or termination of the agreement, if requested by the Parliamentary Protective Service, the Supplier agrees to destroy all documentation and expunge all data received by the Supplier or any officer or servant of the Supplier from the Parliamentary Protective Service during the course of the agreement.

18. INDEPENDENT SUPPLIER

It is the intention of the parties that the agreement is for the performance of services and/or the provision of goods and the Supplier is engaged as an independent Supplier providing services or goods to the Parliamentary Protective Service, and that neither the Supplier nor his/her employees, agents or representatives are engaged as Parliamentary Protective Service employees, and are not subject to the terms and conditions of employment applicable to Parliamentary Protective Service employees.

19. ASSIGNMENT OF AGREEMENT

The agreement may not be assigned, sub-contracted or transferred in any manner by the Supplier without the prior written consent of the Parliamentary Protective Service' Contracting Authority and any assignment, subcontract, or transfer made without that consent is void and of no effect.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

20. **NO IMPLIED OBLIGATIONS**

No implied obligation of any kind by or on behalf of the Parliamentary Protective Service shall arise from anything in the agreement, and the express covenants and agreements herein contained and made by the Parliamentary Protective Service are and shall be the only covenants and agreements upon which any rights against the Parliamentary Protective Service are to be founded; and, without limiting the generality of the foregoing, the agreement supersedes all communications, negotiations and prior arrangements, either written or oral, relating to the work and made prior to the execution date of the agreement.

21. **PERFORMANCE**

The Supplier will report the performance under the agreement to the Parliamentary Protective Service in whatever format and frequency the Parliamentary Protective Service may require.

22. **CONFLICT OF INTEREST**

22.1 No employees of the Parliamentary Protective Service shall be admitted to any share or part of the Framework Agreement or to any benefit arising there from.

22.2 The Supplier must not extend entertainment, gifts, gratuities, discounts or special services regardless of value to Parliamentary Protective Service employees or their families. The Supplier has the responsibility to report to the Parliamentary Protective Service any attempts by Parliamentary Protective Service employees, their families, to obtain such favours.

23. **PUBLIC CEREMONY AND/OR ADVERTISING**

23.1 The Supplier must not allow or permit any public ceremony in connection with the agreement.

23.2 The Supplier must not erect or permit the erection of any sign or advertising.

23.3 The Supplier agrees not to use the name of the Parliamentary Protective Service, or any reference to the Parliamentary Protective Service, in any manner of advertising.

24. **SECURITY REQUIREMENTS**

24.1 Where it is determined by the Parliamentary Protective Service that the Supplier or an employee of the Supplier will have access to Parliamentary Protective Service buildings, or to sensitive information or valuable assets, in the execution of this agreement, prior to the commencement of work the Parliamentary Protective Service may carry out a criminal records name check for any person who has such access.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

24.2   No criminal records check will be carried out without the consent of the person affected. Where consent is refused, the Parliamentary Protective Service reserves the right to determine that this person will not participate in any way in the execution of this agreement.

25. DAMAGES TO PREMISES

25.1 Where the performance of the work requires the presence of the Supplier's personnel on Parliamentary Protective Service premises, the Supplier must take the same care of the premises occupied as it would its own property and will be responsible for any damages to the Parliamentary Protective Service premises or equipment caused by the negligence of its officers, employees, representatives, or agents.

26. INDEMNIFICATION

The Supplier hereby undertakes to save harmless and agrees to indemnify the Parliamentary Protective Service and its employees against any liability whatsoever (including any claims, demands, losses, damages, costs, charges and expenses) that is incurred by the Parliamentary Protective Service and its employees as a direct or indirect result of the conduct of the Supplier, its agents, employees, representatives, or anyone acting on its behalf in the performance of this Contract.

27. PROPRIETARY RIGHTS

All software, data, programs, system documents, research, reports, papers, material and information owned by the Supplier and used in the performance of the services under this agreement are, and will remain, the property of the Supplier, unless otherwise agreed by both parties. All software, data, programs, system documents, research, reports, papers, material, information, trademarks, patents, copyrights and industrial designs arising out of the Supplier's performance of its obligations under this agreement and paid for by the Parliamentary Protective Service under this agreement are the property of the Parliamentary Protective Service and neither the Supplier nor any officer, employee, representative, or agent of the Supplier shall divulge, release, or publish anything related to performance under this agreement without first obtaining the written permission of the Parliamentary Protective Service's Project Authority.

28. LICENCES AND PERMITS

The Supplier will be solely responsible for obtaining from the regulatory authorities under whose jurisdiction it operates and to which it is subject, all approvals, licences, certificates or other requirements connected with the subject matter of this agreement, including licences to use copyrighted software in the performance of the work. The Supplier must, upon request, provide copies of any documents evidencing such approval, licences, certificates or other requirements to the Parliamentary Protective Service's Project Authority.

29. ENVIRONMENTAL PRACTICES

The Supplier shall maintain or exceed the environmental practices indicated in its offer for the duration of the agreement.

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

30. **REPRESENTATION**

The Supplier and the Parliamentary Protective Service shall each appoint a representative to discuss any problems arising pursuant to the provisions contained in the agreement. The representative so appointed by the Parliamentary Protective Service shall be the Parliamentary Protective Service' Project Authority as referred to in this agreement.

31. **PARLIAMENTARY PROTECTIVE SERVICE AUTHORITIES**

The following individuals shall act as the Parliamentary Protective Service's respective authorities:

Project Authority	Contracting Authority
To be completed following agreement award.	**Wayne Dubeau** Senior Procurement Officer Procurement and Contracting Services 155 Queen Street, Office 500 Ottawa, ON K1A 0B8 Tel: (613) 943-4095 Email: wayne.dubeau@pps-spp.parl.gc.ca
Enquiries (Primary Contact) **Wayne Dubeau** Senior Procurement Officer Procurement and Contracting Services 155 Queen Street, Office 500 Ottawa, ON K1A 0B8 Tel: (613) 943-4095 Email: wayne.dubeau@pps-spp.parl.gc.ca	

The preceding authorities may delegate their authority and act through their duly appointed representative.

32. **SUPPLIER REPRESENTATIVES**

The following individuals shall act as the Supplier's representatives:

Contracting Signing Authority	Account Manager (Primary Contact)
To be completed following Agreement Award.	To be completed following Agreement Award.
Other	
To be completed following Agreement Award.	

PPS-RFP-2020-060

CONTINUATION

A – FRAMEWORK AGREEMENT TERMS AND CONDITIONS

33. **NOTICE**

All notices to the Parliamentary Protective Service, including a change to the Supplier's coordinates, must be provided in writing to:

Parliamentary Protective Service
Procurement and Contracting Services
155 Queen Street, #500
Ottawa ON, K1A 0B8
E-mail: Proposals-soumissions@parl.gc.ca

34. **SUBSTITUTION OF PERSONNEL**

34.1   When specific persons have been named in the Supplier's proposal, the Supplier shall provide the services of the persons so named unless the Supplier is unable to do so for reasons beyond its control.

34.2   If at any time the Supplier is unable to provide the services of any specific person named in the agreement, for reasons beyond its control, or if the Parliamentary Protective Service' Project Authority requires the replacement of any individual, the Supplier shall provide a replacement with similar qualifications and experience that is acceptable to the Parliamentary Protective Service' Project Authority.

34.3   The Supplier shall, prior to replacing any specific personnel, give notice to the Parliamentary Protective Service' Project Authority of:

34.3.1   the reason for the removal of the named person from the Work (if such removal was not requested by the Parliamentary Protective Service); and

34.3.2   the name, qualifications and experience of the proposed replacement person.

CONTINUATION

APPENDIX B – PROPOSAL SUBMISSION FORM

1. **BIDDER INFORMATION**

Please fill out the following form, and name one person to be the contact for the proposal and for any clarifications or amendments that might be necessary.	
Bidder Profile:	
Full Legal Name of Bidder*:	
Any Other Relevant Name under Which the Bidder Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Phone Number:	
Fax Number:	
Company Website (If Any):	
RFP Point of Contact:	
RFP Contact Person and Title:	
RFP Contact Phone:	
RFP Contact Facsimile:	
RFP Contact E-mail:	

*In the case of a Consortium or Joint Venture, in addition to indicating who the prime supplier will be, Bidders must name the other parties that comprise the consortium or joint venture and their legal relationship. If Bidders plan to use subcontractors, the names of their subcontractors must be listed as well.

2. **ACKNOWLEDGMENT OF NON-BINDING PROCUREMENT PROCESS**

The Bidder acknowledges that this procurement process will be governed by the terms and conditions of the RFP, and that, among other things, such terms and conditions confirm that this procurement process is not intended to create and does not create a Contract A bidding process nor any contractual or other legally enforceable obligations, and that there will be no legal relationship or obligations created until the Parliamentary Protective Service and the selected Bidder have executed a written agreement.

3. **ABILITY TO PROVIDE DELIVERABLES**

The Bidder has carefully examined the RFP documents and has a clear and comprehensive knowledge of the deliverables required under the RFP. The Bidder represents and warrants its ability to provide the deliverables required under the RFP in accordance with the requirements of the RFP for the prices set out in the Appendix C - Pricing Structure Form. The Bidder has provided a list of any subcontractors to be used to complete the proposed agreement. The Bidder encloses herewith as part of the proposal the mandatory forms set out below:

CONTINUATION

APPENDIX B – PROPOSAL SUBMISSION FORM

FORM	INITIAL TO ACKNOWLEDGE
Proposal Submission Form	
Pricing Structure Form	

Notice to Bidders: There may be forms required in the RFP other than those set out above. See the Mandatory Criteria section of the RFP for a complete listing of mandatory forms.

4.   **NON-BINDING PRICE ESTIMATES**

The Bidder has submitted its prices in accordance with the instructions in the RFP and in the Pricing Structure Form set out in Appendix C. The Bidder confirms that the pricing information provided is accurate. The Bidder acknowledges that any inaccurate, misleading or incomplete information, including withdrawn or altered pricing, could adversely impact the acceptance of its proposal or its eligibility for future work.

5.   **ADDENDA**

The Bidder has read and accepted all addenda issued by the Parliamentary Protective Service. The onus remains on Bidders to make any necessary amendments to their proposal based on the addenda. The Bidder confirms that it has received all addenda by listing the addenda numbers or, if no addenda were issued, by writing the word "None" on the following line:

_____.

6.   **PROHIBITED CONDUCT**

The Bidder declares that it has not engaged in any conduct prohibited under clause 7 of Part 3 – Terms and Conditions of the Procurement Process, Conflict of Interest and Prohibited Conduct.

7.   **CONFLICT OF INTEREST**

For the purposes of this clause, the term "Conflict of Interest" means:

7.1   in relation to the procurement process, the Bidder has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to:

   7.1.1   having, or having access to, confidential information of the Parliamentary Protective Service in the preparation of its proposal that is not available to other Bidders;

   7.1.2   communicating with any person with a view to influencing preferred treatment in the RFP process (including but not limited to the lobbying of decision makers involved in the RFP process); or

   7.1.3   engaging in conduct that compromises, or could be seen to compromise, the integrity of the RFP process; or

CONTINUATION

APPENDIX B – PROPOSAL SUBMISSION FORM

7.2   in relation to the performance of its contractual obligations contemplated in the agreement that is the subject of this procurement, the Bidder's other commitments, relationships or financial interests:

7.2.1   could, or could be seen to, exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgement; or

7.2.2   could, or could be seen to, compromise, impair or be incompatible with the effective performance of its contractual obligations.

If the box below is left blank, the Bidder will be deemed to declare that (a) there was no Conflict of Interest in preparing its proposal; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFP.

Otherwise, if the statement below applies, check the box.

❑   The Bidder declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the Bidder foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFP.

If the Bidder declares an actual or potential Conflict of Interest by marking the box above, the Bidder must set out below details of the actual or potential Conflict of Interest:

_____
_____
_____
_____

The following individuals, as employees, advisors, or in any other capacity (a) participated in the preparation of our proposal; **AND** (b) were employees of the Parliamentary Protective Service and have ceased that employment within twenty-four (24) months prior to the Submission Deadline:

Name of Individual:
Job Classification:
Service Area:
Last Date of Employment with the Parliamentary Protective Service:
Name of Last Supervisor:
Brief Description of Individual's Job Functions:
Brief Description of Nature of Individual's Participation in the Preparation of the Proposal:

(Repeat above for each identified individual)

The Bidder agrees that, upon request, the Bidder will provide the Parliamentary Protective Service with additional information from each individual identified above in the form prescribed by the Parliamentary Protective Service.

CONTINUATION

APPENDIX B – PROPOSAL SUBMISSION FORM

8.   **DISCLOSURE OF INFORMATION**

The Bidder hereby agrees that any information provided in this proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or if required by order of a court or tribunal. The Bidder hereby consents to the disclosure, on a confidential basis, of this proposal by the Parliamentary Protective Service to the Parliamentary Protective Service's advisors retained for the purpose of evaluating or participating in the evaluation of this proposal.

Signature of Witness	Signature of Bidder Representative
Name of Witness	Name and Title
	Date:
	I have authority to bind the Bidder and attest to the accuracy of the information provided in this proposal.

CONTINUATION

APPENDIX C – PRICING STRUCTURE FORM
(Under separate cover)

# CONTINUATION

APPENDIX D – STATEMENT OF REQUIREMENTS

1. BACKGROUND

On June 23, 2015, the Parliamentary Protective Service was created by law under the Parliament of Canada Act. The Speaker of the Senate and the Speaker of the House of Commons are, as the custodians of the powers, privileges, rights and immunities of their respective Houses and of the members of those Houses, responsible for the Service. The newly created parliamentary entity amalgamated the former Senate Protective Service, House of Commons Security Services, and detection specialists, into a single unified security service to serve the Parliament of Canada. While the Director of the Service must be a member of the Royal Canadian Mounted Police (RCMP) by law, he or she has control and management of the daily operations of the organization.

The Director executes his or her mandate under the joint general policy direction of the Speaker of the Senate and the Speaker of the House of Commons. The Speakers of both Houses, being responsible for the Service, and the Minister of Public Safety and Emergency Preparedness have entered into an arrangement to have the RCMP lead the physical security operations of the Service.

2. OBJECTIVE

The PPS requires a Protective Service Dispatch and Reporting System to effectively manage and support key business processes including:
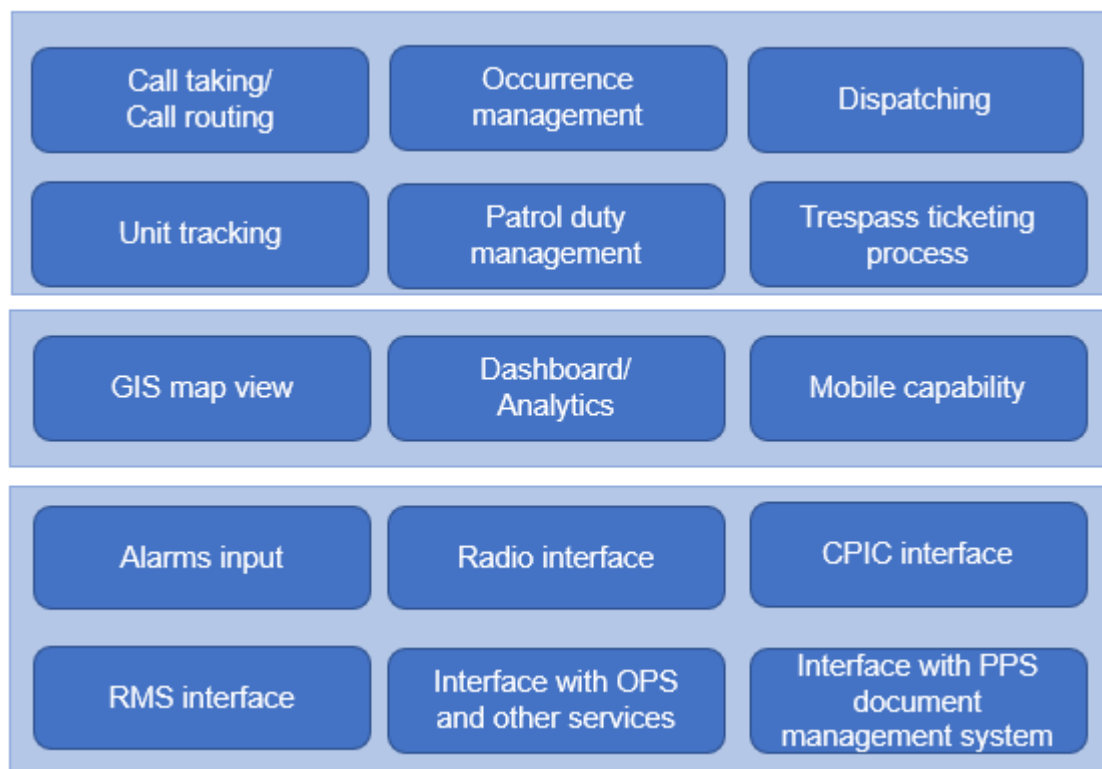
PPS is looking purchase a solution that is modular and can be adapted to the needs of PPS as business processes evolve. The ideal solution may be implemented in phases.

Based on the nature of data to be stored in this solution, the current procurement process is for an on-premise

CONTINUATION

APPENDIX D – STATEMENT OF REQUIREMENTS

solution. The solution may be hosted in the cloud or on-premise in the future. PPS recognizes functional and technical advantages and disadvantages of cloud solutions and is therefore open to learn about possibilities for future consideration. At such time, additional requirements related to cyber security will come into play.

3.   DESCRIPTION OF SCOPE

The following describes the scope of the requirements.

- Implementation and commissioning of a solution and its components meeting the requirements of this document including project management, installation, configuration, data mapping, testing activities, training activities, change management activities and documentation. This may involve interaction with the IT internal hosting/service provider for PPS.
- Solution for approximately 40-45 call taker/dispatchers (10 concurrent users) and 400 (40 concurrent users) units including units at physical posts, on foot and in vehicle.
- Train the trainer approach for
   o   Approximately 15 call taker/dispatchers on all elements of the solution;
   o   Approximately 30 units on the mobile portion of solution;
   o   Approximately 5 supervisors/managers on how to extract and consume information; and
   o   Approximately 3 system administrator / support personnels.
- Ongoing technical support including onsite support during the project and go-live period.
- Costing for annual maintenance and upgrades and / or subscription pricing model.

4.   REQUIREMENTS

4.1   Key terms and definitions used within the statement of requirements:

Term	Definition / Description
BOLO	Be On Lookout. A broadcast issued that typically contains information about a wanted suspect, a person of interest, or a related vehicle.
For your information entry	Similar to a BOLO but lower level of importance.
CPIC	Canadian Police Information Centre.
Occurrence	Event or activity of concern on the Precinct.
Incident Report	Report of occurrence of a significant or emergent nature that occur on the Precinct.
Unit	A PPS employee at a physical post, on foot or in a vehicle.

CONTINUATION

4.2 Categories of requirement

The following presents the structure in which requirements have been categorized.

General Requirements	Call Taking / Occurrence Creation	Dispatch Decision Support	Dispatch Units
Unit Status Management	Occurrence Management	Mobile	Other Operational Requirements
Operational and Statistical Reporting	External and Internal Interfaces	System Administration	Technical Requirements

4.3 Requirements

Respondents should indicate how the proposed solution will meet the following requirements. Respondents are encouraged to present available alternatives in cases where their solution does not meet one of the following requirements, and to include any assumptions made in their response. Please use the tables below to respond:

Item	Requirement	Yes	No	How requirement is Met or Alternative
General Requirements and Professional Services				
GR01	The proposed solution and its components should be fully capable of processing and rendering content in English and French. The English and French rendered should be Canadian English and French. Describe how this works, in terms of language choice, switching languages, screen displays, error messages, reports, documentation, etc. If the proposed solution and its components partially comply to this requirement, describe what functionality is available in both languages and which ones are unilingual.			

CONTINUATION

GR02	Describe training options and recommendations for end-users. Response should address the following: - If English and French instructors and training materials are available; - The type of training offered/available (Webinar, on site, etc.); and - If your offer refresher training to keep important knowledge fresh and current.			
GR03	Describe training options and recommendations for system administrators / support personnel. Response should address the following: - If English and French instructors and training materials are available; - The type of training offer/available (Webinar, on site, at your site, etc.); and - If your offer refresher training to keep important knowledge fresh and current.			
GR04	The vendor should provide knowledge transfer and pertinent documentation to prepare PPS for handling support and configuration post-project implementation. Describe approach for knowledge transfer and typical documentation that will be provided to PPS.			
GR05	The vendor should make available the right resources at the right time to work on different phases of the project. Provide a proposal for a project team structure and describe how the supplier project resources will be deployed over the course of the project and post-implementation. Response should address the following: - Type of resources; and - Resources onsite at PPS premises or offsite. a) The Bidder should provide a CV for each key member of the proposed project team, demonstrating that the experience and qualifications they possess are sufficient to complete this mandate. b) The Bidder should indicate whether each proposed resource is based in Ottawa, or if not, how they will participate in the project.			
GR06	Elaborate on an approach and methodology to			

CONTINUATION

	implement the proposed solution, e.g. gap analysis, design, configure, test, deployment, etc.			
GR07	Describe proposal for project phases, milestones and potential timeline in the form of a Gantt chart.			
GR08	Describe proposed change management approach (e.g. ADKAR, other) and what services will be provided as part of this project.			
GR09	Describe resources required from PPS to ensure project success, including: - Skillset; and - Time percentage or ballpark number of days.			
GR10	Describe options available for post-project support. Response should address the following: - Hours of coverage; - Different levels of incidents and response time; - Escalation procedure; - Whether or not the support can be provided in English, French or both languages; - Level of client's visibility into the incident/defect tracking; and - Whether or not you require certifications on your solution for support personnel. Note that PPS is located in the Eastern time zone and PPS operations are conducted 24/7.			
GR11	Describe the process for clients to request enhancements or changes to the solution so that it can be considered for future releases.			

Call Taking / Occurrence creation

Requirements to support the Call taking business function that consist of receiving the call, obtaining sufficient and accurate information from the caller, determining whether this is a duplicate of an occurrence in progress, recording or updating the occurrence in the CAD system, verifying, analyzing, classifying, and prioritizing the occurrence prior to routing it to the dispatcher when necessary.

Note: A call taker may or may not be the same person as the dispatcher depending on PPS operational requirements at a specific time.

CT01	Ability to create, update and view occurrences with the following information at a minimum: • Date and time • Call taker • Type of Occurrence			

CONTINUATION

	• Origin of a call (Internal, Client, Partner, etc.) • Caller data (Contact information, etc.) • Additional Information such Person data, Vehicle data, Item data (Bag, drone, etc.) as attachments • Location data (different location formats) • Narrative data			
CT02	Describe what other occurrence information can be recorded as part of the default configuration.			
CT03	Describe if and how the proposed solution can be configured to record additional occurrence information that is not part of the default configuration.			
CT04	Ability to create, update and view future-dated occurrences.			
CT05	Ability to generate a unique file number for each occurrence created.			
CT06	Ability to enter various information to classify the occurrence and to assign it a priority to support the dispatch and response needs.			
CT06	Ability to check for duplicate occurrences (within the open or closed occurrences) based on parameters such location and type of occurrence.			
CT07	Ability to verify the location of an occurrence against a valid list of addresses and building names in the system.			
CT08	Ability to translate the occurrence location into another location format. Example: Translating a common place name to an actual civic address Describe options available.			
CT09	Ability to link an occurrence to an another existing occurrence for future retrievability (in case of duplicate occurrences, etc.).			
CT10	Ability to reopen an occurrence.			
CT11	Ability to route new occurrences to dispatchers for handling (occurrence pending queue) using pre-defined business rules.			
CT12	Ability to create an occurrence with an expiry date and time so it can appear in the occurrence log only for a			

CONTINUATION

	certain period of time. Example: an occurrence for awareness purpose.			
Dispatch Decision Support Requirements to support dispatch decision making.				
DD01	Ability to view the occurrence pending queue based on pre-defined business rules.			
DD02	Describe if and how the occurrence pending queue can be configured.			
DD03	Ability to retrieve, from the occurrence pending queue, an occurrence to handle/dispatch.			
DD04	Ability to retrieve recommended unit(s) to dispatch for an occurrence based upon preset criteria such as: • Occurrence type, priority and location of the Occurrence • Proximity of units and unit availability • Unit capability (e.g. skills and equipment required)			
DD05	Ability to override the recommended units for dispatching on an occurrence.			
DD06	Ability to retrieve location hazard and history e.g. relevant historical and tactical information about specific and neighboring locations for decision support. Examples: - Information about previous occurrences at the location - Location has a record of registered firearms - Hazardous materials stored at the location - Relevant medical information concerning residents at the location			
Dispatch Units Requirements around dispatching units and recording receipt acknowledgements from the units.				
DU01	Ability to associate unit(s) dispatched to an occurrence as responding units and to update their unit status accordingly.			
DU02	Ability to identify a unit dispatched on an occurrence as the primary unit.			

CONTINUATION

DU03	Ability to record acknowledgements received from the unit(s) dispatched on an occurrence including timestamp of the update and the user who performed the update.			
DU04	Ability to add/attach information to an occurrence (including specific BOLOs, Hazard information, For your information, etc.) for informing and raising awareness of unit(s) dispatched on an occurrence.			
DU05	Ability for a dispatcher to identify an occurrence as <Situational awareness> and for the system to notify upper management of this situation. (Examples: an arrest, unplanned demo).			
DU06	Ability to reassign unit(s) to a new occurrence and automatically unassign unit(s) from a previous occurrence (previous occurrence back in the pending occurrences queue for handling).			
Unit Status Management Unit status and location must be continually monitored, updated, and recorded by the dispatcher.				
US01	Ability to record any unit status changes along with the timestamp of the update and the user who performed the update. Examples: - Available, 2020-06-26 06:00AM, userabc - Assigned, 2020-06-26 10:26AM, userabc - Unavailable - Lunch, 2020-06-26, 12:01PM, userabc			
US02	Ability to record any unit location changes along with timestamp of the update and the user who performed the update. Examples: - Main Entrance - Victoria, 2020-06-26 06:00AM, user abc - Lounge, 2020-06-26 10:00AM, userdef			
US03	Ability to view / monitor at a glance: • Status of the different units; • The occurrence (occurrence unique identifier, type, priority) on which the each unit is dispatched (if any); and • The location of each unit or their last known location (current occurrence location, last occurrence location, etc.).			

CONTINUATION

US04	Ability to view real-time unit locations - officer on foot or vehicle location. Describe technology and systems required to achieve this. Describe map functionality available for dispatchers, e.g. refresh, ping, zoom, centering.			
US05	Ability to poll/display other geolocation sources on a map (e.g. radios).			
US06	Ability to set the refresh rate for retrieving the real-time unit location and open occurrences on a map.			

Occurrence Management

The occurrence is managed by continually updating the data with any additional information reported by callers or officers on scene. This section addresses these requirements.

OM01	Ability to update the data of an existing occurrence with any additional information reported by callers or units on scene.			
OM02	Ability to efficiently record a log of any preset and miscellaneous actions performed by units /dispatchers on an occurrence along with the timestamp of the update and the user who performed the update. Examples: • Unit 1, En route to location, 2020-04-06 09:33:10, userabc • Unit 1, Arrived at location, 2020-04-06 09:36:17, userabc • Dispatcher, Called ambulance, 2020-04-06 09:38:00, userxyz • Etc. Describe methods used to speed up data entry of actions. (command line, pre-defined set of commands, picklist, etc.).			
OM03	Ability for a dispatcher to set a timer and a comment for a unit, and for the system to notify the dispatcher at expiration of the timer. Describe how the dispatcher would be notified (tone, visual prompt, etc.).			

CONTINUATION

OM04	Ability to attach rich media such document(s), image(s) and video(s) to an occurrence.			
OM05	Ability to close an occurrence with a specific disposition classification/reason. Examples: - False alarm - Resolved			
OM06	Ability to transfer occurrence information to a record management system. Describe how it is done.			
OM07	Ability to provide an occurrence to a group or user for information or analysis purposes.			
Mobile Requirements to support mobile units on foot or in vehicle.				
MO01	Ability to notify Units on their mobile devices when a new occurrence is assigned to them by the dispatcher.			
MO02	Ability for Units to acknowledge receipt of a dispatched occurrence from their mobile device.			
MO03	Ability for Units to retrieve and view an occurrence on a mobile device.			
MO04	Ability for Units to update their status and location from a mobile device. Examples: - Signin, In Vehicle 123 - On duty, Main Entrance - Signout - Not available - Etc.			
MO05	Ability for Units to create and self-assign an occurrence of administrative nature to themselves from a mobile device. Example: Water leak, Patrolling			
MO06	Ability for Units to track their actions on an occurrence from a mobile device using preset actions such as en route, arrived on scene, etc..			
MO07	Ability for the primary unit to close an occurrence from a			

CONTINUATION

	mobile device (with an automatic notification to dispatchers).			
MO08	Ability for Units to attach rich media such as image(s) and video(s) to an occurrence from a mobile device.			
MO09	Ability for Units to search and view BOLO and <For your information> entries from a mobile device.			
MO10	Ability for Units to search and view location and person hazard entries from a mobile device.			
MO11	Ability for Units to create, update, search, attach rich media, view, archive and print Trespass notices in standard Provincial Offence Notice format (electronic ticketing) from a mobile device.			
MO12	Ability for Units to search restricted access person (RAP) list and view details from a mobile device.			
MO13	Ability for Units to view Patrol Routes and Frequency they have been assigned to from a mobile device.			
MO14	The proposed solution on mobile devices should offer a responsive user interface.			
Other Operational Requirements These are operational requirements not specifically related to occurrences.				
OO01	Ability the create, update, publish, search, view, print and archive Be On Lookout (BOLOs) entries with the following information: • Creation date • Created by • Type of BOLO (Person of Interest, etc.) • Expiration date • Priority • Cautions description • Synopsis description • Subject person information • Subject vehicle information • Contact information • Related document(s) / image(s) Note: Printing may require additional privileges.			
OO02	Describe what other BOLO information can be recorded			

CONTINUATION

	as part of the default configuration.			
OO03	Describe if and how the proposed solution can be configured to record additional BOLO information that is not part of the default configuration.			
OO04	Ability to notify users that a new BOLO entry has been published.			
OO05	Ability the create, update, publish, search, view, print and archive <For your information> entries with the following information: • Created Date • Created By • Expiration date • Priority • Title • Description • Related document(s) / image(s)			
OO06	Describe what other <For your information> information can be recorded as part of the default configuration.			
OO07	Describe if and how the proposed solution can be configured to record additional <For your information> information that is not part of the default configuration.			
OO08	Ability to notify users that a new <For your information> entry has been published.			
OO09	If available, ability to create, update, search, attach rich media, view, archive and print Trespass notices in standard Provincial Offence Notice format (electronic ticketing).			
OO10	Ability to create, update, delete, search, attach rich media and view location hazard special condition / requirement / note including an expiry date. Example: location is locked, need special key			
OO11	Ability to create, update, delete, search, attach rich media and view person hazard special condition / requirement / note including an expiry date. Example: mobility restrictions, etc.			
OO12	Ability to create, update, delete, search, attach rich media and view Restricted Access Person (RAP) list.			

CONTINUATION

OO13	Ability to create, update, search and view Patrol Routes and Frequency.			
OO14	Ability to perform Daily Patrol Route Assignment.			
OO15	Ability to search and view Patrol History.			

Operational Reporting

Requirements for reports and dashboard that support the present and immediate operational and statistical reporting requirements based on the information recorded as part of occurrences, unit status and location log information as well as patrol routes, frequency and assignment information.

OR01	Ability to generate, view and print reports related to occurrences to support operational and statistical needs. Describe standard reports that come with the solution by default. Examples: • Daily Log • Activity Analysis (per day of week, hour of the day, per day and hour, etc.) • Response Time Analysis (per location, per time period, etc.) • Time Consumed (per occurrence, per time period, per location, etc.) • Workload activity (per resource, per group, etc.) • Number of Patrols, Number of Demos, in the last 4 years • Average of arrest in regards to demo			
OR02	Describe the analytic capabilities of the proposed solutions to make reporting easier.			
OR03	Ability for end-users to manipulate existing reports and to build their own customized reports. Describe the report functionality including choice of parameters, columns, filtering, sorting, etc. and the ability to save the reports as private or public. Note: If reporting requires any additional software, plug-ins or add-ons, describe the requirement, licensing, training and documentation.			

CONTINUATION

OR04	Ability to export reports in various formats (for example: XLS, CSV, PDF) including the ability to export reports as data only with headers. Describe the export functionality, the different formats available and how the export function treats formatting.			
OR05	Ability to configure and view a dashboard with data visualization capabilities to support operational and management needs. Describe the dashboard functionality. Response should also address the following: - If the dashboard can be tailored to the role of the user - If the user can configure/create their own dashboard (add or remove content)			
OR06	Ability to generate, view and print reports based on to the unit status and location log information. Examples: - Attendance - Who signed in today and at which location - Attendance - Who was present yesterday between 2 and 4PM at West Block			
OR07	Ability to generate, view and print reports based on Patrol Routes, Patrol Frequency and Patrol Assignment.			

External and Internal Interfaces

The proposed solution should be based on open standards/APIs in order to efficiently interface and share information with other systems both internally and externally.

IN01	**CAD to CAD Interface** The proposed solution should be able to interface with CAD solutions from federal, provincial and local agencies and organizations for the purpose of: - Accepting an occurrence from a participating CAD system, in an agreed-upon structure; - Generating and transferring/sharing an occurrence to a peer CAD agency; - Logging all communication between peer agencies; and - Sharing of emergency notifications based on occurrence type and proximity. Response should address the following:			

CONTINUATION

		- Compliance to recognized standards (NIEM, etc.); - Technical means (APIs, etc.) to facilitate data exchange; and - List of CAD solutions that have been interfaced successfully with the proposed solution.		
IN02	**CAD to RMS Interface** The proposed solution should be able to interface with a future Records Management Systems (RMS) solution for the purpose of: - Creating an Incident Report skeleton from CAD occurrence information extracted and transferred to the RMS system; - Inquiring into the RMS data files (e.g., master name index, master location index, etc.) for information that relates to an occurrence. Response should address the following: - Compliance to recognized standards - Technical means (APIs, etc.) to facilitate data exchange - Ability to interface with Cloud RMS provider - List of RMS solutions that have been interfaced successfully with the proposed solution.		
IN03	**Canadian Police Information Centre (CPIC) Interface** The proposed solution **MUST** be able to interface with CPIC to securely query and retrieve: - People information; and - Vehicle information. Response should address the following: - Compliance to recognized standards; and - The method used to securely query and retrieve information from CPIC. Note: Because of the type of information exchanged from and to CPIC, the information cannot flow through corporate emails and must remain in the CAD ecosystem.		
IN04	**Interface with Sharepoint** The proposed solution, on desktop and mobile, should be able to interface with an on premise Sharepoint server (accept hyperlinks) to retrieve and display building / floor plans, standard operating procedures or other documents. Describe how this interface would work.		

CONTINUATION

	Integration with the following document management system: - Microsoft SharePoint Server 2013, 2016 and Online			
IN05	**Interface with Alarm Monitoring Systems** The proposed solution should be able to interface with Alarm Monitoring systems to: - Recognize and accept notification of a specific alarm; - Present alarm information to the call taker; - Create an occurrence based on the alarm information or discard the notification. Example: Interface with Lenel OnGuard system that would trigger the creation of an occurrence when an alarm is received. Please provide a list of Alarm Monitoring systems that have been proven to work well with the proposed solution.			
IN06	**Interface with Mobile Radio system** The proposed solution should be able to interface with mobile radio systems to - Geolocate mapping on emergency activation (duress alarm); - Polling location of mobile radios; and - Display who is transmitting on Push-to-Talk. Example: Motorola P25 System. Please provide a list of Mobile Radio systems that have been proven to work well with the proposed solution.			
IN07	**CTI Interface** Indicate if the proposed solution offers an interface with CTI (computer-telephony integration) and if so, describe it.			
System Administration Requirements to support system administration.				
SA01	**Logging** The proposed solution and its components should log all actions, including CPIC queries, errors, changes, and updates (at the record and field levels, configurable). Logs should be viewable and searchable (Audit tools) by the system administrators.			

CONTINUATION

SA02	**Configurable – User interfaces and Preferences** The proposed solution and its components should be configurable to determine screen parameters, color choices, font size, screen layout, and user preferences.			
SA03	**Configurable – Branding** The proposed solution and its components should be configurable to match the Parliamentary Protective Service brand (logos, colors). Describe what can be configured for that purpose.			
SA04	**Configurable – Content** The proposed solution and its components should allow the configuration of content such as labels, error messages and help. Describe how this can be accomplished and to what extent it is possible to do so.			
SA05	**Table Maintenance** The proposed solution and its components should provide the ability for PPS to maintain the data used to support system recommendations, decisions and etc. Examples: - Units; - Occurrence types; - Occurrence priorities; - Etc. Describe if there is any import/export functionality to add, update and delete entries as part these tables. Describe if there is the possibility to create custom attributes.			
SA06	**Geofile Maintenance** The proposed solution and its components should provide the ability for PPS the maintain a geofile and its layers. Describe the following: - The process by which PPS could obtain GIS information and how it is updated in the solution - If there are costs involved with mapping and address file upkeep; - The mapping platform (open source or not); - Whether or not we can enter and update additional layers and how.			

PPS-RFP-2020-060

CONTINUATION

Technical Requirements Requirements that the propose solution and its components should address / comply with.				
TR01	**On-Premise Installation** All software components and data should reside on the Canadian Parliamentary premise.			
TR02	**Desktop Operating System Compatibility** All desktop components should run on the standard desktop operating systems and be forward compatible. Compatibility with the current Microsoft Windows 10 64-bit and with future feature releases.			
TR03	**Server Operating System Compatibility** All server components should run on Microsoft Windows Server 2016 64-bit and be forward compatible.			
TR04	**Administrative Rights** All software components should not require user accounts to have Windows Administrator rights in order to run. This excludes installation, configuration and upgrade operations, which may require administrator rights. All system components must work with User Account Control (UAC) enabled.			
TR05	**Database Engine Compatibility** All database components should be hosted and run natively on the standard database management system (DBMS) and without compatibility mode enabled. Compatibility with the following database management system is required: - Microsoft SQL Server 2016 64-bit			
TR06	**Server Hardware Compatibility** All server components should operate with no performance or functional degradation using the standard server hardware configuration. Server hardware configuration: - Virtual Machine running under Microsoft Hyper-V; - Storage Area Network (SAN); and - Network: 1 Gbps.			
TR07	**External Licencing Server** All software components should not require a			

CONTINUATION

	connection to an external licencing server in order to run. This excludes installation, configuration and upgrade operations, which may require a temporary licensing server connection.			
TR08	**System Components Full Disclosure** The vendor should provide a full disclosure of all the system prerequisites and components (third-party components, open source components, embedded components, etc.) with their dependencies and versions.			
TR09	**Deployment in Multiple Environments** The system should allow multiple instances to run simultaneously in multiple environments: production, lab test, demo, training, development etc. (one instance per environment, with each environment hosted on its own set of servers).			
TR10	**License Management and Renewal** The vendor should describe the Licence Management and Renewal process (if any) and how license consumption is determined (user based, concurrent licenses, etc.).			
TR11	**Mail Server** If software components utilize e-mail messaging, it should use the Exchange mail server to send e-mail. Integration with the following mail server is required: - Microsoft Exchange Server 2013 - Compatible with Exchange Online			

TR12	**Secure Messaging Services**
	The system should provide a way to securely transmit unit-to-unit messaging, unit-to-dispatcher messaging and external messaging to other agencies (different than corporate email services).
	Examples:
	   - CAD to CAD
	   - CPIC to CPIC			

TR13	**System Security** The system must be secured through authentication and authorization. All communications must be done through secure protocols (such as SSL or TLS). Authorization: Role based authority to grant or deny access to certain screens/functions within the system.			
TR14	**Mobile Devices**			

CONTINUATION

	If mobile functionality is provided using a mobile/tablet device, then it should be compatible with the standard mobile operating systems. The current standard mobile operating systems are iOS 10 or Android 9 or above. Communication with the main software using 4G or better and using corporate Wi-Fi.			
TR15	**Mobile Application Deployment** iOS and Android Apps should be able to be managed by Intune MDM system. Apps may also be built for Ad-Hoc or Enterprise distribution and meet the required criteria to be managed by Intune MDM.			
TR16	**Support and Maintenance** Previous versions of vendor supplied software should continue to be covered under the Support and Maintenance Agreement for a minimum of 2 major releases.			
TR17	**Product Lifecycle** The vendor should have a defined process to keep the system prerequisites and components up-to-date with the latest security patches, and to advise customers on the availability of those patches.			
TR18	**Mobile Security** Data in transit from mobile device to Parliamentary network should be encrypted.			
TR19	**Customization** The vendor will not propose any functionality that requires customization of the licensed product.			
TR20	**Web Hosting Platform Compatibility** All Web components should run natively on the Parliamentary Web hosting platforms. Compatibility with the following Web server platform is required: - Microsoft Internet Information Server 10.0 or later.			
TR21	**Data Export/Import between Environments** The system should allow data to be exported/imported across environments. The export/import should include master data, business and user data, personalization, configurations and customizations.			

CONTINUATION

TR22	**Upgrades - Migration and Custom Configurations** The system design should support migration of all the custom modules, configurations and personalization such as the custom event handlers, custom workflows, custom plugins, reports, fields, user profiles, queries, workflows, tasks, views, security (roles, users, permissions) etc. from the previous version of the system to the new version of the system without losing or breaking existing functionality. Tools should be provided to identify potential migration issues.			
TR23	**Installation and Upgrade** The system installation and upgrade for both client and server components should be documented and should run with minimal effort and manual interventions. The vendor should provide the following system installation and upgrade documentation and tools: - Installation and migration Documentation; - Installation/upgrade setup file(s) for the server components; - Installation/upgrade setup file(s) for the client components; - Scriptable installation/upgrade; - Migration scripts or tools from vendor to help migrating from a previous version to the new version; and - Changes required to operating system settings (firewall, file permissions, registries, etc.) should be documented.			
TR24	**Support for Last Versions** The system components should support at least the last two major versions of Microsoft desktop and server operating systems, Microsoft database management systems and related third-party components.			
TR25	**Interface with external applications (receive information from external application)** The system should provide built-in interfaces (API) to allow external applications to create, read, update and delete system records, and to execute operations (such as execute a workflow, execute a task, etc.). The provided interfaces should be documented, supported and maintained by the vendor. The system should be extensible and use open APIs and SDKs in order to support future in-house development. All APIs and SDKs should be fully documented and supported by the vendors.			
TR26	**Interface with External Applications (send information to external application)**			

CONTINUATION

	The system should provide built-in interfaces (API) to send messages and data to external applications. The provided interfaces should be documented, supported and maintained by the vendor. The system should use open APIs and SDKs. All APIs and SDKs should be fully documented and supported by the vendors.			
TR27	**Server-Based Report Generation System** All reporting modules should integrate with the Parliamentary server-based report generation system. Integration with the following server-based report generation system is required: - Microsoft SQL Server 2016 reporting services.			
TR28	**Application Data Security** All software components should provide data security mechanisms restricting unauthorized access and preventing tampering of stored data. In addition, the system should allow to restrict data access at the record level, field level based on the authenticated user and/or related user roles.			
TR29	**System Security** The system components should be secured and designed in a way to be protected against the common attacks/vulnerabilities.			
TR30	**System architecture** The system should be based on a multi-tier architecture to separate the data, application and Web tiers. For development\testing purpose, it should be possible to install all the tiers on a single server. Provide architectural diagram(s) of the proposed solution, indicating technical architecture, functional modularization, embedded API's, interaction with GIS software and external interfaces.			
TR31	**Concurrency (Number of Connections)** All software components should function with no performance or functional degradation when 100 client users or external application connections are using the system.			
TR32	**Load Balancing** All server components should support working with hardware load balancing and high availability without performance and functionality impacts.			
TR33	**Transaction Rollback**			

CONTINUATION

	If a fault occurs during a long running transaction, the system should undo or resume the transaction, issue an alert and log the transaction error.			
TR34	**SAN** The system should allow using Storage Area Network (SAN) technology for data storage needs.			
TR35	**Redundancy** The system should provide multiple levels of system redundancy with failover capabilities for all server and database components, allowing for uninterrupted operation in case of failure of the primary system. All major subsystems should be capable of automatically re-routing communications to alternate server components without operator intervention.			
TR36	**Tolerance to Network Loss** The system should be tolerant to and gracefully survive (does not crash or require restart) network connectivity loss. Restoration of network connectivity should not cause system restart, component restart or performance degradation compared to a normal operation scenario.			
TR37	**System Self-Diagnostics** The system should provide comprehensive self-diagnostics messages for all its components. Critical self-diagnostics results can be sent as alerts, e-mail, SMS and/or windows event log entries. The self-diagnostics tests can be run on a configurable periodic basis and/or on request.			
TR38	**Single Sign On / User Credentials / Timeout** The solution should support both Single Sign On (SSO) and entry of user credentials, based on PPS preference, as a configurable option. Describe also, whether a session timeout is a configurable option.			
TR39	**Directory Service** All software components requiring user authentication should be integrated with the Parliamentary directory service. HoC Directory Service: -Microsoft Active Directory (LDAP).			
TR40	**Vendor Remote Access** The vendor should explain whether they will require			

CONTINUATION

	access to the installed system using remote tools, to support the installation or for post project support. If yes, what tool(s) does the bidder recommend?			
TR41	**Secure User Remote Access** The vendor should explain whether they provide user secure access to support remote work. If yes, what tools does the vendor recommend?			
TR42	**Protocols, Ports and Firewall** The vendor should provide a description of Protocols, Ports and firewall requirements for their system.			

TR43	**Product roadmap**
	Provide 3-year system roadmap, including planned additional business functionalities, technical features, support future versions of operating systems, database management systems and related third-party components, any plans towards cloud computing and plans for alliances with other software solutions.
	
	If software is currently available for both on-premise and cloud, provide this information:
	   - Since what month/year has the cloud version been commercially available
	   - What percentage of current clients uses the on-premise version and the cloud version
	   - Does the supplier have a timeframe for phasing out the on-premise version.			

TR44	**Client upgrade process**
	Describe typical process for clients to embark on major release upgrades. For example:
	   - How much time should be planned for major upgrades (duration)
	   - Is the software cost included in maintenance fee
	   - Are supplier's professional services included or an extra fee
	   - Does the above apply, should the upgrade be from on-premise to the supplier's cloud offering
	   - If required, will the supplier move client's data from the on-premise database to the cloud database.			

TR45	**System performance and limitations** a) Describe what mechanisms and techniques are utilized within the system to ensure quick response time for users. b) Describe whether there are any thresholds on volume of data, upon which system performance			

CONTINUATION

	may start to degrade (e.g. 5 years of data; # of occurrences, etc.) c) Explain best practices the client may employ to ensure the system operates at optimum performance and d) Describe services offered by the supplier to put those practices in place.			

CONTINUATION

CONTINUATION

APPENDIX E – EVALUATION CRITERIA AND COMPLIANCE MATRIX

Bidders must meet a minimum pass mark of 70% on the technical score in order to be considered further.

The technical score will account for 80% of the bidder's overall evaluated score in this RFP.

1. REQUIREMENTS DESCRIPTION

Bidders shall provide detailed responses as to how their solution meets the requirements, as described in section 4.3 of APPENDIX D – STATEMENT OF REQUIREMENTS for every section, as described below:

- General Requirements and Professional Services: GR01-GR11

- Call Taking/ Occurrence Creation: CT01-CT-12

- Dispatch Decision Support: DD01-DD06

- Dispatch Units: DU01-DU06

- Unit Status Management: US01-US06

- Occurrence Management: OM01-OM07

- Mobile: MO01-MO14

- Other Operational Requirements: OO01-OO15

- Operational Reporting: OR01-OR07

- External and Internal Interfaces: IN01-IN07

- System Administration: SA01-SA06

- Technical Requirements: TR01-TR45

CONTINUATION

APPENDIX E – EVALUATION CRITERIA AND COMPLIANCE MATRIX

2.   CORPORATE PROFILE AND PROJECT SUMMARIES

#	Description of Criterion	Bidder's Proposal Reference (compliance matrix)
R1	**Corporate Profile** The Bidder shall provide information on the following: a) How widely used is the proposed solution? - Provide a list of the organizations currently using the solution - Number of organizations by country - Types of organizations - Approximately how many employees use the solution/in which language b) What experience does the firm have in delivering in our specific industry, namely: - Protective Security and Law Enforcement, - Public Sector Agencies. c) How long has the vendor been in business? d) Age of proposed solution? e) Are you developers and/or resellers of the proposed solution? f) Are you based in Canada?	

CONTINUATION

APPENDIX E – EVALUATION CRITERIA AND COMPLIANCE MATRIX

R2	**Project Summaries**	

	Using the Template in Appendix F, the Bidder shall provide three (3) written project summaries describing in detail installations/configurations/deployments of their proposed solution, on behalf of client organizations during the past three (3) years. Project Summaries will be evaluated based on the extent to which they are similar and relevant to the PPS' requirement, described in the Statement of Requirements, and PPS' operating environment.
	
	Within each project summary provided, the Bidder should indicate (a-l):
	  a) Name of the client organization to whom the solution was sold/deployed;
	  b) The number of licences and the licensing model;
	  c) Was the proposed solution deployed on premise or in the cloud;
	  d) A description of the modules that were deployed (similar to PPS requirement);
	  e) A description of the activities that the Bidder was responsible for in the deployment of the proposed solution;
	  f) Excerpt from the Training plan
	  g) Deployment Approach and Methodology
	  h) A description of the extent to which the solution was configured, without necessitating additional effort due to customization;
	  i) Dates/duration of the project;
	  j) The support model provided;
	  k) Results and extent to which it was deployed on time, on budget, and met the expectations of the client; and
	  l) Name, address, telephone number of the client project authority to whom the Bidder reported.
	
	The PPS reserves the right to contact the named client project authorities for the purpose of verifying the accuracy and veracity of the information provided in the Bidder's Proposal. Should the PPS choose to contact the project authorities and should one (1) or more named client project authorities provide a negative reference regarding the accuracy or veracity of the Bidder's proposal, the proposal may be deemed non-compliant and given no further consideration.
	Failure to provide all the above information with respect to each cited project summary may render the Bidder's proposal non-compliant.	

CONTINUATION

PPS-RFP-2020-060

CONTINUATION

APPENDIX F – PROJECT SUMMARY TEMPLATE

Project Reference #: _____	
A) Name of the client organization to whom the solution was sold/deployed;	
Client:	
B) The number of licences and the licensing model.	
C) Was the proposed solution deployed on premise or in the cloud.	
D) Please describe the modules that were deployed (similar to PPS requirement).	
E) Please describe the activities that the Bidder was responsible for in the deployment of the proposed solution.	
F) Please describe an Excerpt from the Training plan.	
G) Please describe the Deployment Approach and Methodology.	
H) Please describe the extent to which the solution was configured, without necessitating additional effort due to customization.	
I) Please provide the dates/duration of the project.	
J) Please describe the support model provided.	
K) Please describe The Results and extent to which it was deployed on time, on budget, and met the expectations of the client	
L) Client Project Authority:	
Name:	
Address:	
Telephone Number:	
Email Address:	