REPUBLIC OF KENYA

PARLIAMENT OF KENYA

PARLIAMENTARY SERVICE COMMISSION (PSC)

PARLIAMENT BUILDINGS, PARLIAMENT ROAD
P.O. BOX 41842 00100, Nairobi
Tel: +254 020 2221291
Email: dg@parliament.go.ke
Website: www.parliament.go.ke

TENDER DOCUMENT

TENDER NO: PJS/017/2019-2020

FOR

SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF A NEXT-GENERATION FIREWALL

TENDER CLOSING DATE:

FRIDAY, 29TH MAY, 2020 AT 1100AM

TABLE OF CONTENTS

SECTION I - INVITATION TO TENDER

Date: 8th May, 2020

To: M/s

RE: TENDER NO. PJS/017/2019-2020 FOR SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF A NEXT-GENERATION FIREWALL

The Parliamentary Service Commission invites sealed bids from eligible tenderers for the Supply, Delivery, Installation, Testing, Training and Commissioning of a Next-Generation Firewall for three years.

Interested eligible tenderers may obtain further information from the **Procurement Office on 2nd Floor, Protection House, Nairobi.** A complete set of the Tender Document may be downloaded free of charge from the **Commission's Website; www.parliament.go.ke** or IFMIS Portal; **www.supplier.treasury.go.ke.** Tenderers may seek clarifications through **procurementpjs@parliament.go.ke** or **dg@parliament.go.ke.**

Duly completed, serialized and paginated tender documents (original and copy) and a softcopy of the same are to be enclosed in plain sealed envelopes, marked with the **tender number**, **name** and **as prescribed under this Tender document** and be dropped in the **Tender Box** at the **Reception on 2nd Floor, Protection House, Nairobi** or be addressed to:

Director General, Parliamentary Joint Services,
Parliamentary Service Commission,
Parliament Buildings,
P.O. Box 41842 00100,
NAIROBI, KENYA.

so as to be received on or before **Friday, 29th May, 2020** at **11.00 a.m.**

Tenders will be opened immediately thereafter in the presence of the Candidates who choose to attend or their appointed representatives, at **Protection House, 2nd Floor Boardroom**, Nairobi.

Tenders must be accompanied by a tender Security of **Kshs. 100,000.00** valid for 150 days from the date of tender opening in form of a bank guarantee from a reputable bank or guarantee from an insurance company approved by the Public Procurement Regulatory Authority (PPRA) payable to Parliamentary Service Commission.

Prices quoted should be inclusive of all taxes and delivery costs, and must be in Kenya Shillings and shall remain valid for **120 days** from the closing date of the tender.

DIRECTOR GENERAL, PARLIAMENTARY JOINT SERVICES,
PARLIAMENTARY SERVICE COMMISSION

SECTION II – INSTRUCTIONS TO TENDERERS

TABLE OF CONTENTS. **Page**

SECTION II: INSTRUCTIONS TO TENDERERS

2.1 Eligible tenderers

2.1.1. This Invitation to tender is open to all tenderers eligible as described in the instructions to tenderers. Successful tenderers shall provide the services for the stipulated duration from the date of commencement (hereinafter referred to as the term) specified in the tender documents.

2.1.2. The Commission's employees, Committee members, Board members and their relatives (spouse and children) are not eligible to participate in the tender.

2.1.3. Tenderers shall provide the qualification information statement that the tenderer (including all members, of a joint venture and subcontractors) is not associated, or have been associated in the past, directly or indirectly, with a firm or any of its affiliates which have been engaged by the Commission to provide consulting services for the preparation of the design, specifications, and other documents to be used for the procurement of the services under this Invitation for tenders.

2.1.4 Tenderers involved in corrupt or fraudulent practices or debarred from participating in public procurement shall not be eligible.

2.2 Cost of tendering

2.2.1 The Tenderer shall bear all costs associated with the preparation and submission of its tender, and the Commission, will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.

2.2.2 The price to be charged for the tender document shall be Kshs. 1,000.00.

2.2.3 The Commission shall allow the tenderer to review the tender document free of charge before purchase.

2.3 Contents of tender documents

2.3.1. The tender document comprises of the documents listed below and addenda issued in accordance with these instructions to tenders: -

i) Instructions to tenderers
ii) General Conditions of Contract
iii) Special Conditions of Contract
iv) Schedule of Requirements

v) Description of services to be offered
vi) Form of tender
vii) Price schedules
viii) Contract form
ix) Mandatory Confidential Business Questionnaire Form
x) Performance security form

2.3.2. The Tenderer is expected to examine all instructions, forms, terms, and specifications in the tender documents. Failure to furnish all information required by the tender documents or to submit a tender not substantially responsive to the tender documents in every respect will be at the tenderers risk and may result in the rejection of its tender.

2.4 Clarification of Documents

2.4.1. A prospective candidate making inquiries of the tender document may notify the Commission in writing or by post, fax or email at the entity's address indicated in the Invitation for tenders. The Commission will respond in writing to any request for clarification of the tender documents, which it receives no later than seven (7) days prior to the deadline for the submission of tenders, prescribed by the Commission. Written copies of the Procuring entities response (including an explanation of the query but without identifying the source of inquiry) will be sent to all prospective tenderers who have received the tender documents"

2.4.2. The Commission shall reply to any clarifications sought by the tenderer within 3 days of receiving the request to enable the tenderer to make timely submission of its tender.

2.5 Amendment of documents

2.5.1. At any time prior to the deadline for submission of tenders, the Commission, for any reason, whether at its own initiative or in response to a clarification requested by a prospective tenderer, may modify the tender documents by issuing an addendum.

2.5.2. All prospective tenderers who have obtained the tender documents will be notified of the amendment by post, fax or email and such amendment will be binding on them.

2.5.3. In order to allow prospective tenderers reasonable time in which to take the amendment into account in preparing their tenders, the Commission, at its discretion, may extend the deadline for the submission of tenders.

2.6 Language of tender

2.6.1. The tender prepared by the tenderer, as well as all correspondence and documents relating to the tender exchanged by the tenderer and the Commission, shall be written in English language. Any printed literature furnished by the tenderer may be written in another language provided they are accompanied by an accurate English translation of the relevant passages in which case, for purposes of interpretation of the tender, the English translation shall govern.

2.7 Documents Comprising the Tender

The tender prepared by the tenderer shall comprise the following components: -

a) A Tender Form and a Price Schedule completed accordingly. Documentary evidence established that the tenderer is eligible to tender and is qualified to perform the contract if its tender is accepted;
b) Tender security as prescribed
c) Mandatory Confidential Business Questionnaire

2.8 Form of Tender

2.8.1 The tenderers shall complete the Form of Tender and the appropriate Price Schedule furnished in the tender documents, indicating the services to be performed.

2.9 Tender Prices

2.9.1 The tenderer shall indicate on the Price schedule the unit prices where applicable and total tender prices of the services it proposes to provide under the contract.

2.9.2 Prices indicated on the Price Schedule shall be the cost of the services quoted including all customs duties and VAT and other taxes payable:

2.9.3 Prices quoted by the tenderer shall remain fixed during the term of the contract unless otherwise agreed by the parties. A tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

2.9.4 Contract price variations shall not be allowed for contracts not exceeding one year (12 months).

2.9.5 Where contract price variation is allowed, the variation shall not exceed 10% of the original contract price.

2.9.6 Price variation requests shall be processed by the Commission within 30 days of receiving the request.

2.10 Tender Currencies

2.10.1 Prices shall be quoted in Kenya Shillings unless otherwise specified in the appendix to in Instructions to Tenderers.

2.11 Tenderers Eligibility and Qualifications.

2.11.1 The tenderer shall furnish, as part of its tender, documents establishing the tenderers eligibility to tender and its qualifications to perform the contract if its tender is accepted.

2.11.2 The documentary evidence of the tenderers qualifications to perform the contract if its tender is accepted shall establish to the Commission's satisfaction that the tenderer has the financial and technical capability necessary to perform the contract.

2.12 Tender Security

2.12.1 The tenderer shall furnish, as part of its tender, a tender security for the amount and form specified in the Invitation to tender.

2.12.2 The tender security shall be in the amount as prescribed in the instructions to tenderers.

2.12.3 The tender security is required to protect the Commission against the risk of Tenderer's conduct which would warrant the security's forfeiture.

2.12.4 The tender security shall be denominated in a Kenya Shillings or in another freely convertible currency and shall be in the form of:

a) A bank guarantees.
b) Cash.
c) Such insurance guarantee approved by the Authority.
d) Letter of credit

2.12.4 Any tender not secured will be rejected by the Commission as non-responsive.

2.12.5 Unsuccessful tenderer's security will be discharged or returned as promptly as possible but not later than thirty (30) days after the expiration of the period of tender validity prescribed by the Commission.

2.12.6 The successful tenderer's tender security will be discharged upon the tenderer signing the contract and furnishing the performance security.

2.12.7 The tender security may be forfeited:

(a) If a tenderer withdraws its tender during the period of tender validity specified by the procuring entity on the Tender Form; or

(b) In the case of a successful tenderer, *if* the tenderer fails:

(i) to sign the contract.

or

(ii) to furnish performance security

(c) If the tenderer rejects, correction of an error in the tender.

2.13 Validity of Tenders

2.13.1 Tenders shall remain valid for 120 days or as specified in the invitation to tender after date of tender opening prescribed by the Commission. A tender valid for a shorter period shall be rejected by the Commission as non-responsive.

2.13.2 In exceptional circumstances, the Commission may solicit the Tenderer's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The tender security provided shall also be suitably extended. A tenderer may refuse the request without forfeiting its tender security. A tenderer granting the request will not be required nor permitted to modify its tender.

2.14 Format and Signing of Tenders.

2.14.1 The tenderer shall prepare two copies of the tender, clearly / marking each "ORIGINAL TENDER" and "COPY OF TENDER," as appropriate. In the event of any discrepancy between them, the original shall govern.

2.14.2 The original and all copies of the tender shall be typed or written in indelible ink and shall be signed by the tenderer or a person or persons duly authorized to bind the tenderer to the contract. All pages of the tender, except for unamended printed literature, shall be initialed by the person or persons signing the tender.

2.14.3 The tender shall have no interlineations, erasures, or overwriting except as necessary to correct errors made by the tenderer, in which case such corrections shall be initialed by the person or persons signing the tender.

2.15 Sealing and Marking of Tenders

2.15.1 The tenderer shall seal the original and the copy of the tender in separate envelopes, duly marking the envelopes as "ORIGINAL TENDER" and "COPY OF TENDER". The envelopes shall then be sealed in an outer envelope.

2.15.2 The inner and outer envelope shall:

(a) be addressed to the Commission at the address given in the Invitation to Tender.

(b) bear tender number and name in the invitation to tender and the words, "DO NOT OPEN BEFORE" the date and time of closing indicated in the Appendix of Instructions To Tenderers.

2.15.3 The outer envelopes shall also indicate the name and address of the tenderer to enable the tender to be returned unopened in case it is declared "late".

2.15.4 If the outer envelope is not sealed and marked as required, Commission will assume no responsibility for the tender's misplacement or premature opening.

2.15 Deadline for Submission of Tenders

2.16.1 Tenders must be received by the Commission at the address specified under paragraph 2.15.2 no later than **Friday, 29th May, 2020 at 11.00 a.m.**

2.16.2 The Commission may, at its discretion, extend this deadline for the submission of tenders by amending the tender documents in accordingly, in which case all rights and obligations of the Commission and candidates previously subject to the deadline will thereafter be subject to the deadline as extended.

2.16.3 Bulky tenders which will not fit in the tender box shall be received by the Commission as provided for in the appendix.

2.17 Modification and withdrawal of tenders

2.17.1 The tenderer may modify or withdraw its tender after the tender's submission, provided that written notice of the modification, including substitution or withdrawal of the tender's is received by the Commission prior to the deadline prescribed for the submission of tenders.

2.17.2 The Tenderer's modification or withdrawal notice shall be prepared, sealed, marked, and dispatched accordingly. A withdrawal notice may also be sent by cable, but followed by a signed confirmation copy, postmarked not later than the deadline for submission of tenders.

2.17.3 No tender may be modified after the deadline for submission of tenders.

2.17.4 No tender may be withdrawn in the interval between the deadline for submission of tenders and the expiration of the period of tender validity specified by the tenderer on the Tender Form. Withdrawal of a tender during this interval may result in the Tenderer's forfeiture of its tender security.

2.17.5 The Commission may at any time terminate procurement proceedings before contract award and shall not be liable to any person for the termination.

2.17.6 The Commission shall give prompt notice of the termination to the tenderers and on request give its reasons for termination within 14 days of receiving the request from any tenderer.

2.18 Opening of Tenders

2.18.1 The Commission will open all tenders in the presence of tenderers' representatives who choose to attend, at **11.00 am** on **Friday 29th May, 2020** and in the location specified in the invitation to tender. The tenderers' representatives who are present shall sign a register evidencing their attendance.

2.18.3 The tenderers' names, tender modifications or withdrawals, tender prices, discounts, and the presence or absence of requisite tender security and such other details as the Commission, at its discretion, may consider appropriate, will be announced at the opening.

2.18.4 The Commission will prepare minutes of the tender opening which will be submitted to the tenderers that signed the tender opening register and will have made the request.

2.19 Clarification of tenders

2.19.1 To assist in the examination, evaluation and comparison of tenders the Commission may at its discretion, ask the tenderer for a clarification of its tender. The request for clarification and the response shall be in writing, and no change in the prices or substance shall be sought, offered, or permitted.

2.19.2 Any effort by the tenderer to influence the Commission in the Commission's tender evaluation, tender comparison or contract award decisions may result in the rejection of the tenderers tender.

2.20 Preliminary Examination and Responsiveness

2.20.1 The Commission will examine the tenders to determine whether they are complete, whether any computational errors have been made, whether required securities have been furnished whether the documents have been properly signed, and whether the tenders are generally in order.

2.20.2 Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If the candidate does not accept the correction of the errors, its tender will be rejected, and its tender security may be forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.

2.20.3 The Commission may waive any minor informality or nonconformity or irregularity in a tender which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any tenderer.

2.20.4 Prior to the detailed evaluation, the Commission will determine the substantial responsiveness of each tender to the tender documents. For purposes of these paragraphs, a substantially responsive tender is one which conforms to all the terms and conditions of the tender documents without material deviations. The Commission's determination of a tender's responsiveness is to be based on the contents of the tender itself without recourse to extrinsic evidence.

2.20.5 If a tender is not substantially responsive, it will be rejected by the Commission and may not subsequently be made responsive by the tenderer by correction of the nonconformity.

2.21 Conversion to a single currency

2.21.1 Where other currencies are used, the Commission will convert those currencies to Kenya shillings using the selling exchange rate on the date of tender closing provided by the central bank of Kenya.

2.22 Evaluation and comparison of tenders.

2.22.1 The Commission will evaluate and compare the tenders which have been determined to be substantially responsive.

2.22.2 The comparison shall be of the price including all costs as well as duties and taxes payable on all the materials to be used in the provision of the services.

2.22.3 The Commission's evaluation of a tender will take into account, in addition to the tender price, the following factors, in the manner and to the extent indicated in the technical specifications:

(a) Operational plan proposed in the tender;
(b) deviations in payment schedule from that specified in the Special Conditions of Contract;

2.22.4 The following evaluation methods will be applied:-

(a) ***Operational Plan.***
The Commission requires that the services under the Invitation for Tenders shall be performed at the time specified in the Schedule of Requirements. Tenders offering to perform longer than the Commission's required delivery time will be treated as non-responsive and rejected.

(b) ***Deviation in payment schedule.***
Tenderers shall state their tender price for the payment on a schedule outlined in the special conditions of contract. Tenders will be evaluated on the basis of this base price. Tenderers are, however, permitted to state an alternative payment schedule and indicate the reduction in tender price they wish to offer for such alternative payment schedule. The Commission may consider the alternative payment schedule offered by the selected tenderer.

2.22.5 The Tender Evaluation Committee shall evaluate the tender within the prescribed period from the date of opening the tender.

2.22.6 To qualify for contract awards, the tenderer shall have the following:-

(a) Necessary qualifications, capability experience, services, equipment and facilities to provide what is being procured.
(b) Legal capacity to enter into a contract for procurement
(c) Shall not be insolvent, in receivership, bankrupt or in the process of being wound up and is not the subject of legal proceedings relating to the foregoing
(d) Shall not be debarred from participating in public procurement.

2.23. Contacting the Commission

2.23.1 No tenderer shall contact the Commission on any matter relating to its tender, from the time of the tender opening to the time the contract is awarded.

2.23.2 Any effort by a tenderer to influence the Commission in its decisions on tender evaluation tender comparison or contract award may result in the rejection of the tenderers tender.

2.24 Award of Contract

a) Post qualification

2.24.1 In the absence of pre-qualification, the Commission will determine to its satisfaction whether the tenderer that is selected as having submitted the lowest evaluated responsive tender is qualified to perform the contract satisfactorily.

2.24.2 The determination will take into account the tenderer's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the tenderers qualifications submitted by the tenderer as well as such other information as the Commission deems necessary and appropriate.

2.24.3 An affirmative determination will be a prerequisite for award of the contract to the tenderer. A negative determination will result in rejection of the Tenderer's tender, in which event the Commission will proceed to the next lowest evaluated tender to make a similar determination of that Tenderer's capabilities to perform satisfactorily.

b) Award Criteria

2.24.3 The Commission will award the contract to the successful tenderer whose tender has been determined to be substantially responsive and has been determined to be the lowest evaluated tender, provided further that the

tenderer is determined to be qualified to perform the contract satisfactorily.

2.24.4 The Commission reserves the right to accept or reject any tender and to annul the tendering process and reject all tenders at any time prior to contract award, without thereby incurring any liability to the affected tenderer or tenderers or any obligation to inform the affected tenderer or tenderers of the grounds for the Commission's action. If the Commission determines that none of the tenderers is responsive; the Commission shall notify each tenderer who submitted a tender.

2.24.5 A tenderer who gives false information in the tender document about its qualification or who refuses to enter into a contract after notification of contract award shall be considered for debarment from participating in future public procurement.

2.25 Notification of award

2.25.1 Prior to the expiration of the period of tender validity, the Commission will notify the successful tenderer in writing that its tender has been accepted.

2.25.2 The notification of award will signify the formation of the Contract subject to the signing of the contract between the tenderer and the Commission. Simultaneously the other tenderers shall be notified that their tenders have not been successful.

2.25.3 Upon the successful Tenderer's furnishing of the performance security, the Commission will promptly notify each unsuccessful Tenderer and will discharge its tender security.

2.26 Signing of Contract

2.26.1 At the same time as the Commission notifies the successful tenderer that its tender has been accepted, the Commission will simultaneously inform the other tenderers that their tenders have not been successful.

2.26.2 Within seven (7) days of receipt of the Contract Form, the successful tenderer shall sign and date the contract and return it to the Commission.

2.26.3 The parties to the contract shall have it signed within 30 days from the date of notification of contract award unless there is an administrative review request.

2.27 Performance Security

2.27.1 Within thirty (30) days of the receipt of notification of award from the Commission, the successful tenderer shall furnish the performance security in accordance with the Conditions of Contract, in the Performance Security

Form provided in the tender documents, or in another form acceptable to the Commission.

2.27.2 Failure of the successful tenderer to comply with the requirement shall constitute sufficient grounds for the annulment of the award and forfeiture of the tender security, in which event the Commission may make the award to the next lowest evaluated or call for new tenders.

2.28 Corrupt or Fraudulent Practices

2.28.1 The Commission requires that tenderers observe the highest standard of ethics during the procurement process and execution of contracts. A tenderer shall sign a declaration that he has not and will not be involved in corrupt or fraudulent practices.

2.28.2 The Commission will reject a proposal for award if it determines that the tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question;

2.28.3 Further, a tenderer who is found to have indulged in corrupt or fraudulent practices risks being debarred from participating in public procurement in Kenya.

APPENDIX TO INSTRUCTIONS TO THE TENDERERS

The following information for procurement of services shall complement or amend the provisions of the instructions to tenderers. Wherever there is a conflict between the provisions of the instructions to tenderers and the provisions of the appendix, the provisions of the appendix herein shall prevail over those of the instructions to tenderers

Instructions to tenderers	Particulars of appendix to instructions to tenderers
2.1	Particulars of eligible tenderers: **All eligible candidates**
2.2.2	Price to be charged for tender documents. **Kshs. 0.00**
2.10.1	Particulars of other currencies allowed. **The prices quoted shall be in Kenya Shillings only**
2.11	Particulars of eligibility and qualifications documents of evidence required. • **Submission of two (2) sealed envelopes (separate technical and financial bids)** • **Submission of all the documentation and requirements as outlined in the Schedule of Requirements on page 25 and as per the submission format prescribed.** • **Compliance to the evaluation criteria as specified on page 28 of this document**
2.12.2	Tender Security of **Kshs.100,000.00** from a reputable bank or insurance company approved by Public Procurement Regulatory Authority (PPRA) valid for **150 days** from the date of tender closing in form a Bank guarantee from a reputable bank registered with the Central Bank of Kenya in the attached prescribed format.
2.16.3	Bulky tenders which will not fit in the tender box shall be delivered and received at the Procurement Office on 2nd floor, Protection House, Nairobi
2.22.1	The evaluation and comparison of tenders will be as indicated under Section V (Schedule of requirements)
2.24	Particulars of post – qualification if applicable. **N/A**
2.27	Particulars of performance security if applicable**. N/A**
Clarification	For any clarification on this tender, please write to**:** **Director General, Parliamentary Joint Services** **Parliamentary Service Commission** **P. O. Box 41842 00100** **NAIROBI** At least seven (7) days before the tender closing date

SECTION III - GENERAL CONDITIONS OF CONTRACT

TABLE OF CONTENTS **Page**

GENERAL CONDITIONS OF CONTRACT

3.1 Definitions

In this contract the following terms shall be interpreted as indicated:

a) "The contract" means the agreement entered into between the Commission and the tenderer as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
b) "The Contract Price" means the price payable to the tenderer under the Contract for the full and proper performance of its contractual obligations.
c) "The services" means services to be provided by the contractor including materials and incidentals which the tenderer is required to provide to the Commission under the Contract.
d) "The Commission" means the organization sourcing for the services under this Contract.
e) "The contractor means the individual or firm providing the services under this Contract.
f) "GCC" means general conditions of contract contained in this section
g) "SCC" means the special conditions of contract
h) "Day" means calendar day

3.2 Application

These General Conditions shall apply to the extent that they are not superceded by provisions of other part of contract.

3.3 Standards

3.3.1 The services provided under this Contract shall conform to the standards mentioned in the Schedule of requirements.

3.4 Patent Right's

The tenderer shall indemnify the Commission against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the services under the contract or any part thereof.

3.5 Performance Security.

3.5.1 Within fourteen (14) days of receipt of the notification of Contract award, the successful tenderer shall furnish to the Commission the performance security where applicable in the amount specified in Special Conditions of Contract.

3.5.2 The proceeds of the performance security shall be payable to the Commission as compensation for any loss resulting from the Tenderer's failure to complete its obligations under the Contract.

3.5.3 The performance security shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Commission and shall be in the form of:

a) Cash.
b) A bank guarantees.
c) Such insurance guarantee approved by the PPOA
d) Letter of credit.

3.5.4 The performance security will be discharged by the Commission and returned to the candidate not later than thirty (30) days following the date of completion of the tenderer's performance of obligations under the contract, including any warranty obligations under the contract.

3.6 Inspections and Tests

3.6.1 The Commission or its representative shall have the right to inspect and/or to test the services to confirm their conformity to the Contract specifications. The Commission shall notify the tenderer in writing, in a timely manner, of the identity of any representatives retained for these purposes.

3.6.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s). If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Commission.

3.6.3 Should any inspected or tested services fail to conform to the Specifications, the Commission may reject the services, and the tenderer shall either replace the rejected services or make alterations necessary to meet specification requirements free of cost to the Commission.

3.6.4 Nothing in paragraph 3.7 shall in any way release the tenderer from any warranty or other obligations under this Contract.

3.7 Payment

3.7.1 The method and conditions of payment to be made to the tenderer under this Contract shall be specified in SCC.

3.8 Prices

3.8.1 Prices charged by the contractor for services performed under the Contract shall not, with the exception of any Price adjustments authorized in SCC, vary from the prices by the tenderer in its tender or in the Commission's request for tender validity extension as the case may be. No variation in or modification to the terms of the contract shall be made except by written amendment signed by the parties.

3.9 Assignment

3.9.1 The tenderer shall not assign, in whole or in part, its obligations to perform under this contract, except with the Commission's prior written consent.

3.10 Termination for Default

3.10.1 The Commission may, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the tenderer, terminate this Contract in whole or in part:

a) if the tenderer fails to provide any or all of the services within the period(s) specified in the Contract, or within any extension thereof granted by the Commission.

b) if the tenderer fails to perform any other obligation(s) under the Contract.

c) if the tenderer, in the judgment of the Commission has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

3.10.2 In the event the Commission terminates the Contract in whole or in part, it may procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered, and the tenderer shall be liable to the Commission for any excess costs for such similar services.

3.11 Termination of insolvency

The Commission may at the anytime terminate the contract by giving written notice to the contractor if the contractor becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the contractor, provided that such termination will not produce or affect any right of action or remedy, which has accrued or will accrue thereafter to the Commission.

3.12 Termination for convenience

3.12.1 The Commission by written notice sent to the contractor may terminate the contract in whole or in part, at any time for its convenience. The notice of termination shall specify that the termination is for the Commission convenience, the extent to which performance of the contractor of the contract is terminated and the date on which such termination becomes effective.

3.12.2 For the remaining part of the contract after termination the Commission may elect to cancel the services and pay to the contractor on agreed amount for partially completed services.

3.13 Resolution of disputes

3.13.1 The Commission's and the contractor shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute arising between them under or in connection with the contract.

3.13.2 If after thirty (30) days from the commencement of such informal negotiations both parties have been unable to resolve amicably a contract dispute either party may require that the dispute be referred for resolution to the formal mechanisms specified in the SCC.

3.14 Governing Language

3.14.1 The contract shall be written in the English language. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in the same language.

3.15 Force Majeure

3.15.1 The contractor shall not be liable *for* forfeiture of its performance security, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

3.16 Applicable Law.

The contract shall be interpreted in accordance with the laws of Kenya unless otherwise specified in the SCC.

3.17 Notices

Any notices given by one party to the other pursuant to this contract shall be sent to the other party by post or by fax or E-mail and confirmed in writing to the other party's address specified in the SCC.

A notice shall be effective when delivered or on the notices effective date, whichever is later.

SECTION IV - SPECIAL CONDITIONS OF CONTRACT

4.1 Special conditions of contract shall supplement the general conditions of contract, wherever there is a conflict between the GCC and the SCC, the provisions of the SCC herein shall prevail over those in the GCC.

4.2 Special conditions of contract with reference to the general conditions of contract.

General conditions of contract reference	Special conditions of contract
3.5	Specify performance security if applicable: **N/A**
3.7	Specify method Payments. **Payment to be made upon satisfactory installation of the firewall.**
3.7	All payments shall be in Kenya Shillings and there shall be no advance payment. There shall be no payment of interest on delayed payments.
3.8	Specify price adjustments allowed. **None**
3.13	Specify resolution of disputes. **Disputes to be settled as per the Arbitration Laws of Kenya**
3.13.1	Any dispute arising out of the Contract that cannot be amicably resolved between the parties shall be referred by either party to the arbitration and a final decision by a panel of a person to be agreed between the parties. Failing agreement on the appointment of an Arbitrator, the Arbitrator shall be appointed by the Chairperson of the Chartered Institute of Arbitrators-Kenya branch on the request of the applying party. The seat of arbitration shall be in Kenya.
3.13.2	Delete "thirty (30) days" Replace with "Sixty (60) days"
3.16	Specify applicable law. **Laws of Kenya**
3.17	Indicate addresses of both parties. **Client:** **Director General, Parliamentary Joint Service** **Parliamentary Service Commission** **P. O. Box 41842 00100** **NAIROBI**
Other's as necessary	Complete as necessary

SECTION V – SCHEDULE OF REQUIREMENTS

A. CONTRACT DURATION

The Contract will run for a period of three years from the commencement date subject to satisfactory performance.

B. FIRM'S QUALIFICATION REQUIREMENTS

Prospective Bidders must meet the following: -

MANDATORY QUALIFICATION REQUIREMENTS
Prospective Bidders MUST:-

I. Preliminary Evaluation

1) Submit an original and copy of each bid.
2) Attach a copy of the Certificate of Registration/Incorporation.
3) Attach a copy of a valid Tax Compliance Certificate from KRA
4) Attach a bid security of Kshs.100,000.00 valid for 150 days from the date of tender opening and shall be from a Reputable Bank or Insurance Company approved by PPRA.
5) Submit fully filled, signed and stamped attached Mandatory Confidential Business Questionnaire
6) Submit duly filled, signed and stamped Form of Tender.
7) Presentation of the tender document including all attachments in a logical manner. The document should be serialised and paginated including all attachments.
8) Evidence in form of recommendation letters of having successfully provided similar services to at least three (3) institutions (attach a current signed recommendation letter in client's letterhead and each recommendation to be supported by a duly executed LPO/contract from the same institution).
9) Attach copies of audited accounts for the last three years, 2016, 2017, 2018.
10) Declaration that that the firm has not been debarred from participating in public procurement proceedings (Declaration must be commissioned by Commissioner for Oath). Declaration that the firm is not guilty of any violation of fair employment laws and practices (Declaration must be commissioned by Magistrate/Commissioner for Oath/Notary Public).

II. Technical Qualification Requirements

No.	Item	Technical Requirements	Complied/ Not Complied
1.	Firewall Specifications	Must support a minimum of 2 x 40GE QSFP+ Slots, 4 x 25GE SFP28 slots, 4 x 10GE SFP+ slots populated with 4 10G SFP+ SR modules, 8 x GE RJ45 ports and 8 x GE SFP slots	
		Must support at least 8 Million Maximum Concurrent Sessions	
		Must support at least 500,000 New Sessions/Second	
		Must support at least 70Gbps of firewall throughput	
		Must be a leader in the latest Gartner Network Firewall Quadrant	
		Must support at least 12 Gbps Enterprise/Production IPS Throughput	
		Must support at least 10 Gbps SSL Inspection Throughput	
		Must support at least 7 Gbps Enterprise/Production Threat Protection Throughput	
		Must support at least 960GB SSD storage	
		Must be supplied with at least 2000 SSL VPN licenses	
		Must support dual hot swappable power supply units	
		Must have the following licenses included Application Control, IPS, AV, Mobile Security, DNS Filtering, Web Filtering and Sandbox	
2.	Stateful Firewall Features	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model	
		The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP	
		Solution must include the ability to work in Transparent/Bridge mode	
		The Firewall must provide NAT functionality, including PAT.	
		Must support "Policy-based NAT"	
		Firewall must support Voice based protocols like H.323, SIP, SCCP, MGCP etc. and RTP Pin holing.	
		IPv6 support for both NAT and Transparent Mode	
3.	Authentication Features	Support for RSA SecureID or other Token based products	
		Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication	
		Support for Native Windows Active Directory or Novell eDirectory Integration	

No.	Item	Technical Requirements	Complied/ Not Complied
		Must support authentication based on LDAP Groups	
		Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators	
		Support for authentication at the firewall policy level (Local and Remote)	
4.	VPN Features	The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS	
		Must support the following protocols: - DES & 3DES MD5, SHA-1 & the more secure SHA-256 authentication Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14. Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)	
		Must support Hub and Spoke VPN topology, must also support PPTP and L2TP over IPSec VPN protocols.	
		IPSec NAT Traversal & Dead Peer Detection Must be supported	
		IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.	
		Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy	
		Must support SSL Two-factor Authentication with Digital Certificates	
		Must support Single Sign-On Bookmarks for SSL Web VPN.	
		Must support NAT within IPSec/SSL VPN tunnels	
		Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser-based access)	
5.	High Availability	The device must support Active-Active as well as Active-Passive redundancy.	
		The Firewall must support stateful failover for both Firewall and VPN sessions.	
		The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor	
		Must support VRRP and Link Failure Control	
6.	Datacenter Optimization Features	Must have support for WCCP and ICAP protocols	
		Must support Server Load Balancing with features like HTTP persistence	

No.	Item	Technical Requirements	Complied/ Not Complied
		Must support TCP Multiplexing	
		Must support HTTPS Offloading with flexible Digital Certificate Management	
7.	Management Features	Support for Image upgrade via FTP, TFTP and WebUI	
		The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management	
		Must have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (i.e. Trusted Hosts for Management)	
		There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)	
		The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).	
		Provision to generate automatic notification of events via mails / syslog	
		Provision to send alerts to multiple email recipients	
		Support for role-based administration of firewall	
		Must support simultaneous login of Multiple Administrators.	
		Must have provision to customize the dashboard (e.g.: by selecting suitable Widgets)	
		The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP	
		Must support system software rollback to the previous version after upgrade	
8.	Intrusion Prevention Features	Must have a built-in Signature and Anomaly based IPS engine on the same unit	
		Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.	
		Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc.	
		Must have protection for 3000+ signatures	
		Able to prevent denial of service and Distributed Denial of Service attacks.	
		Must be able to exclude certain hosts from scanning of particular signatures	
		Supports CVE-cross referencing of threats where applicable.	
		Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment	
		Must support granular tuning with option to configure Overrides	

No.	Item	Technical Requirements	Complied/ Not Complied
		for individual signatures.	
		Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)	
		Supports attack recognition inside IPv6 encapsulated packets.	
		Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.	
		Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options	
		Must offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses	
		Must Identify and control over 1000+ applications (i.e. Application control feature)	
		Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc	
9.	Sandboxing Technology	The solution Must be tightly integrated with the cloud threat mitigation in order to make the protection more effective and updated so as to minimize the occurrence of false positives.	
		The solution must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.	
		The solution Must be able to inspect the web session to detect and notify the malicious web activity including malicious file downloads through the web/internet.	
		The solution Must be able to store payload and artifacts of the detected threats for further analysis and incident time lines that is with the third party as well.	
		The proposed solution Must have the ability to analyze, detect and block malware in common file formats including but not limited to executable, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.	
		The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution Must also assign a unique identification number to each identified/detected threat for future reference.	
		The solution shall detect the entire infection lifecycle and provide	

No.	Item	Technical Requirements	Complied/ Not Complied
		stage-by-stage analysis of the attack starting from system exploitation to data exfiltration	
		The solution Must be part of an integrated model therefore it Must interact with other security network element in order to give full proof detection and correction model rather than having a point product.	
		The solution must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures.	
		The solution must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions	
		The solution must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.	
		The solution must have ability to block all outbound call- back communication initiated by the internal clients (infected)	
10.	Antimalware Features	The appliance must facilitate embedded anti-virus support which is ICSA Labs certified	
		Must include Antispyware and Worm Prevention	
		Must have option to schedule automatic updates of the new virus pattern.	
		Gateway AV Must be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM	
		Must have configurable policy options to select what traffic to scan for viruses	
		Must have option to configure to respond to virus detection at the gateway in several ways i.e. Delete the file, Alert email, Quarantine etc.	
		Must have options to prevent user downloads based on file extension as well as file type	
		Must have support for "Flow-Based Antivirus Scanning Mode" for high throughput requirements	
		The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus	
		Must have an ability of Antivirus scanning for IPv6 traffic	
11.	Web Filtering Features	The appliance Must facilitate embedded Web Content Filtering feature	
		Web content filtering solution must work independently without the need to integrate with External proxy server.	

No.	Item	Technical Requirements	Complied/ Not Complied
		Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.	
		URL database Must have more than 2 billion URLs under 70+ categories.	
		Must be able to block different categories/sites based on User Authentication.	
		Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.	
		Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable	
		Must have options to customize the "Blocked Webpage Message" information displayed to end users	
		Must have facility to schedule the configurations so that non-work-related sites are blocked during office hours and allow access to all sites except harmful sites during non-office hrs. Must also have time-based quota	
		The solution Must have options to block java applets, ActiveX as well as cookies	
		The solution Must be able to block URLs hosting spywares / adware etc.	
		Must have configurable policy options to define the URL exempt list	
12.	Traffic Optimization Features	Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover	
		Must support multi-path intelligence using rules defined by: Source address and/or user group Destination address and/or a selection of over 3,000 applications Path selection using particular link quality criteria or SLAs defined	
		Must support traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support	
		Must support an option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces	
		Must support traffic shaping policies that assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.	
		Must support DSCP match in SD-WAN rules	

No.	Item	Technical Requirements	Complied/ Not Complied
		Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support	
		Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols	
		Must support multiple WAN optimization sessions on the same tunnel, must support zero-touch deployment	
13.	Additional Requirements	The solution must be appliance based and Must facilitate multi-application environment.	
		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations	
		The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW mode.	
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.	
		Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host-based licenses.	
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).	
		Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other.	
		Must support more than one ISP with automatic ISP failover	
		Must have support for Explicit Proxy and Transparent Proxy	
		Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions	
		Must provide integrations to different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on your network in real time including 3rd party security products	
		Responsive/ Not Responsive	

Note: These are the minimum specifications and bidders have to comply with them to proceed to the next stage of evaluation.

TECHNICAL QUALIFICATION REQUIREMENTS

A. Profile of the firm providing;

- Details of its physical address, contact details, directorship, clients including the organizational structure.

- ❖ Brief indication of the proposed staff for this assignment, position and their specific duties/ responsibilities in the assignment as either team leader or other technical staff.

B. The firm

- o Provide a list of its five (5) major clients, contract values and contact persons in those client's organizations.
- o Provide evidence in form of duly signed recommendation letters by Clients/customers of having undertaken and completed at least three (3) similar service contracts of similar nature, complexity and magnitude of (over Kshs.1,000,000.00). Satisfactory past performance by the clients shall be a critical consideration for this assignment.

C. Qualifications of personnel

Submit at **least three (3) CVs of the technical personnel** who should have qualifications and experience as follows: -

Team leader

- ❖ At least a Bachelor's Degree in ICT related field from a recognized University or College.
- ❖ At least 3yrs related work experience at a senior level in a big Organization.
- ❖ Membership in professional bodies/Association.

Other technical (2No.)

- ❖ At least a Diploma in ICT related field from a recognized University or College.
- ❖ At least 2yrs related work experience in a big Organization.

D. A written proposal that provides the following details: -

- ❖ Proposed implementation schedule/work plan for the assignment;
- ❖ Proposed approach and methodology in delivering the service and outputs at each stage.

C. EVALUATION CRITERIA.

The following will be the evaluation criteria: -

STAGE 1: PRELIMINARY EVALUATION/ EVALUATION ON THE MANDATORY QUALIFICATION REQUIREMENTS

- The firm must meet all the mandatory qualification requirements as listed above and shall be evaluated on '***YES' OR 'NO' BASIS*** and any bid that does not meet any of the mandatory requirements shall be disqualified from detailed technical evaluation.

STAGE 2: DETAILED EVALUATION: EVALUATION ON THE TECHNICAL QUALIFICATION REQUIREMENTS

Evaluation Criteria (Total of 100 points);-

a) Profile of the firm **[Maximum 20 points];**
b) Qualification of the firm **[Maximum 30 points];**
c) Qualification of staff **[Maximum 30 points];**
d) Proposed implementation schedule /work plan & methodology **[Maximum 20 points];**

100 points

In order to qualify for further financial consideration the firm must score a minimum of **80 points**.

STAGE 3: FINANCIAL EVALUATION

Tenderers should note that only tenders that score 80% and above on the technical evaluation will qualify to have their financial bids evaluated. Those scoring below 80% will not be evaluated further and will be disqualified.
The following documents shall be confirmed to be duly filled:

a) Form of tender
b) Price schedule

The financial ranking of the will them be done to determine the lowest in cost bid.

STAGE 4: **RECOMMENDATION FOR AWARD**

The technically responsive and lowest in cost bid shall be recommended for award of the contract.

SECTION VI - DESCRIPTION OF SERVICES

1.0 INTRODUCTION

The Parliamentary Service Commission intends to identify and contract a reputable and competent firm to supply, deliver, install, testing, Training and commissioning of a Next-Generation Firewall for a period of three (3) years.

2.0 SCOPE OF THE SERVICES

The successful bidder shall supply, delivery, installation, testing, Training and commissioning of a Next-Generation Firewall with the following minimum specifications:

No.	Item	Technical Requirements
1.	Firewall Specifications	Must support a minimum of 2 x 40GE QSFP+ Slots, 4 x 25GE SFP28 slots, 4 x 10GE SFP+ slots populated with 4 10G SFP+ SR modules, 8 x GE RJ45 ports and 8 x GE SFP slots
		Must support at least 8 Million Maximum Concurrent Sessions
		Must support at least 500,000 New Sessions/Second
		Must support at least 70Gbps of firewall throughput
		Must be a leader in the latest Gartner Network Firewall Quadrant
		Must support at least 12 Gbps Enterprise/Production IPS Throughput
		Must support at least 10 Gbps SSL Inspection Throughput
		Must support at least 7 Gbps Enterprise/Production Threat Protection Throughput
		Must support at least 960GB SSD storage
		Must be supplied with at least 2000 SSL VPN licenses
		Must support dual hot swappable power supply units
		Must have the following licenses included Application Control, IPS, AV, Mobile Security, DNS Filtering, Web Filtering and Sandbox
2.	Stateful Firewall Features	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model
		The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP
		Solution must include the ability to work in Transparent/Bridge mode
		The Firewall must provide NAT functionality, including PAT.
		Must support "Policy-based NAT"

No.	Item	Technical Requirements
		Firewall must support Voice based protocols like H.323, SIP, SCCP, MGCP etc. and RTP Pin holing.
		IPv6 support for both NAT and Transparent Mode
3.	Authentication Features	Support for RSA SecureID or other Token based products
		Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication
		Support for Native Windows Active Directory or Novell eDirectory Integration
		Must support authentication based on LDAP Groups
		Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators
		Support for authentication at the firewall policy level (Local and Remote)
4.	VPN Features	The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS
		Must support the following protocols: - DES & 3DES MD5, SHA-1 & the more secure SHA-256 authentication Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14. Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)
		Must support Hub and Spoke VPN topology, must also support PPTP and L2TP over IPSec VPN protocols.
		IPSec NAT Traversal & Dead Peer Detection Must be supported
		IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.
		Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy
		Must support SSL Two-factor Authentication with Digital Certificates
		Must support Single Sign-On Bookmarks for SSL Web VPN.
		Must support NAT within IPSec/SSL VPN tunnels
		Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser-based access)
5.	High Availability	The device must support Active-Active as well as Active-Passive redundancy.
		The Firewall must support stateful failover for both Firewall and VPN sessions.
		The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor

No.	Item	Technical Requirements
		Must support VRRP and Link Failure Control
6.	Datacenter Optimization Features	Must have support for WCCP and ICAP protocols
		Must support Server Load Balancing with features like HTTP persistence
		Must support TCP Multiplexing
		Must support HTTPS Offloading with flexible Digital Certificate Management
7.	Management Features	Support for Image upgrade via FTP, TFTP and WebUI
		The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management
		Must have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (i.e. Trusted Hosts for Management)
		There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)
		The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).
		Provision to generate automatic notification of events via mails / syslog
		Provision to send alerts to multiple email recipients
		Support for role-based administration of firewall
		Must support simultaneous login of Multiple Administrators.
		Must have provision to customize the dashboard (e.g.: by selecting suitable Widgets)
		The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP
		Must support system software rollback to the previous version after upgrade
8.	Intrusion Prevention Features	Must have a built-in Signature and Anomaly based IPS engine on the same unit
		Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.
		Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc.
		Must have protection for 3000+ signatures
		Able to prevent denial of service and Distributed Denial of Service attacks.
		Must be able to exclude certain hosts from scanning of particular signatures
		Supports CVE-cross referencing of threats where applicable.
		Must provide the facility to configure Profile based sensors

No.	Item	Technical Requirements
		(Client/Server) for ease of deployment
		Must support granular tuning with option to configure Overrides for individual signatures.
		Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)
		Supports attack recognition inside IPv6 encapsulated packets.
		Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.
		Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options
		Must offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses
		Must Identify and control over 1000+ applications (i.e. Application control feature)
		Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc
9.	Sandboxing Technology	The solution Must be tightly integrated with the cloud threat mitigation in order to make the protection more effective and updated so as to minimize the occurrence of false positives.
		The solution must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.
		The solution Must be able to inspect the web session to detect and notify the malicious web activity including malicious file downloads through the web/internet.
		The solution Must be able to store payload and artifacts of the detected threats for further analysis and incident time lines that is with the third party as well.
		The proposed solution Must have the ability to analyze, detect and block malware in common file formats including but not limited to executable, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.
		The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution Must also assign a unique identification number to each identified/detected threat for future reference.
		The solution shall detect the entire infection lifecycle and provide

No.	Item	Technical Requirements
		stage-by-stage analysis of the attack starting from system exploitation to data exfiltration
		The solution Must be part of an integrated model therefore it Must interact with other security network element in order to give full proof detection and correction model rather than having a point product.
		The solution must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures.
		The solution must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions
		The solution must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.
		The solution must have ability to block all outbound call- back communication initiated by the internal clients (infected)
10.	Antimalware Features	The appliance must facilitate embedded anti-virus support which is ICSA Labs certified
		Must include Antispyware and Worm Prevention
		Must have option to schedule automatic updates of the new virus pattern.
		Gateway AV Must be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM
		Must have configurable policy options to select what traffic to scan for viruses
		Must have option to configure to respond to virus detection at the gateway in several ways i.e. Delete the file, Alert email, Quarantine etc.
		Must have options to prevent user downloads based on file extension as well as file type
		Must have support for "Flow-Based Antivirus Scanning Mode" for high throughput requirements
		The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus
		Must have an ability of Antivirus scanning for IPv6 traffic
11.	Web Filtering Features	The appliance Must facilitate embedded Web Content Filtering feature
		Web content filtering solution must work independently without the need to integrate with External proxy server.
		Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.

No.	Item	Technical Requirements
		URL database Must have more than 2 billion URLs under 70+ categories.
		Must be able to block different categories/sites based on User Authentication.
		Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.
		Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable
		Must have options to customize the "Blocked Webpage Message" information displayed to end users
		Must have facility to schedule the configurations so that non-work-related sites are blocked during office hours and allow access to all sites except harmful sites during non-office hrs. Must also have time-based quota
		The solution Must have options to block java applets, ActiveX as well as cookies
		The solution Must be able to block URLs hosting spywares / adware etc.
		Must have configurable policy options to define the URL exempt list
12.	Traffic Optimization Features	Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover
		Must support multi-path intelligence using rules defined by: Source address and/or user group Destination address and/or a selection of over 3,000 applications Path selection using particular link quality criteria or SLAs defined
		Must support traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support
		Must support an option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces
		Must support traffic shaping policies that assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.
		Must support DSCP match in SD-WAN rules
		Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support
		Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols
		Must support multiple WAN optimization sessions on the same

No.	Item	Technical Requirements
		tunnel, must support zero-touch deployment
13.	Additional Requirements	The solution must be appliance based and Must facilitate multi-application environment.
		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations
		The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW mode.
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.
		Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host-based licenses.
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).
		Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other.
		Must support more than one ISP with automatic ISP failover
		Must have support for Explicit Proxy and Transparent Proxy
		Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions
		Must provide integrations to different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on your network in real time including 3rd party security products

3.0 PERSONNEL REQUIREMENTS

The provision of the services shall require the service provider to avail trained personnel to support the Client on need basis.

The personnel shall not include anyone on attachment from the service provider. In case the service provider wishes to add some third personnel, Parliament shall be notified in writing and the request approved by the immediate supervisor.

In case of personnel change, the new personnel identifications and curriculum vitae shall have to be provided and verified by the immediate supervisor before they report to work on behalf of the service provider.

The personnel shall be at all times be officially dressed and adhered to the code of conduct of Parliament staff. They shall at all times wear identification badges provided.

4.0 PERSONNEL QUALIFICATION

The personnel should ideally possess the following qualifications: -

- ❖ At least a Degree in ICT related field from a recognized University or College.
- ❖ Adequate work experience (more than 5 years) in provision of similar services.

5.0 WORKING EQUIPMENT

The Service provider is required to possess standard maintenance working equipment at all times and maintain them at their cost.

7.0 ESSENTIAL DUTIES AND RESPONSIBILITIES OF THE CLIENT

i. PSC will endeavor to provide as much information and documentation required and sufficient for the contractor PSC will provide a work station on need basis
ii. PSC will provide copies of existing relevant reports and documents.
iii. PSC will nominate a liaison officer who will maintain regular contact with the providers on matters regarding this assignment.
iv. PSC will provide appropriate administrative support to the team
v. PSC will provide Gate passes as necessary

9.0 GENERAL CONTRACT TERMS

a) The successful firm will start the services immediately following the completion of the procurement process and as specified in the Contract

b) An agreement will be drawn detailing the levels of engagement between the parties.

c) The assignment will be for three years duration from the date of commencement or as specified in the agreement or any such other period as mutually agreed by the parties in writing.

d) The rates quoted will remain in force for the full period of the contract. No demand for revision of rates or variation on any account shall be entered during the contract period unless where there is proportional increase or decrease in the scope of services.

e) The service provider shall operate as per specified guidelines and follow all documentation procedures as mentioned by the Commission.

f) If the services provided by the contractual service provider are not found to be satisfactory, one-month advance notice shall be provided before the termination of the contract.

g) In event the service contractor does not carry out the services as scheduled or on any emergency call, the Client would terminate the contract in terms of the provisions herein.

10.0 TERMS OF PAYMENT

a) The successful bidder will be paid on submission of certified invoices, worksheets/job cards and any other supporting documentation or as agreed during the Negotiation Meeting between the parties.

b) The Commission will endeavor to pay within thirty (30) days from the date of submission of certified invoices and worksheets/job cards acceptable to the Commission.

SECTION VII - STANDARD FORMS

Notes on the standard Forms

1. **Form of Tender** -The form of Tender must be completed by the tenderer and submitted with the tender documents. It must be duly signed by duly authorized representatives of the tenderer.

2. **Price Schedule Form**-The price schedule form must similarly be completed and submitted with the tender. It must be duly signed by duly authorized representatives of the tenderer.

3. **Tender declaration form-** -The tender declaration form must similarly be completed as prescribed. It must also be duly signed by duly authorized representatives of the tenderer.

4. **Confidential Business Questionnaire Form** - This form must be completed as prescribed by the tenderer and submitted with the tender documents.

5. **Contract Form** -The contract form shall not be completed by the tenderer at the time of submitting the tender. The contract form shall be completed after contract award and should incorporate the accepted contract price.

6. **Performance security Form** - The performance security form should not be completed by the tenderer at the time of tender preparation. Only the successful tenderer will be required to provide performance security in the form provided herein or in another form acceptable to the Commission.

7. **Attachments**

    - Appendix A: Sample letter of offer

1. FORM OF TENDER

Date_____
Tender No._____

To……..
……..
[Name and address of Commission]
Gentlemen and/or Ladies:

1. Having examined the tender documents including Addenda Nos.. *[insert numbers,* the of which is hereby duly acknowledged, we the undersigned, offer to provide.
   [Provision of Internet Services services] in conformity with the said tender documents for the sum of Kshs.……
   ……
   ……..*[total tender amount in words and figures]* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Tender.
2. We undertake, if our Tender is accepted, to provide the services in accordance with the services schedule specified in the Schedule of Requirements and details of service.
3. If our Tender is accepted, we will obtain the tender guarantee in a sum equivalent to _____ percent of the Contract Price for the due performance of the Contract, in the form prescribed by (Commission).
4. We agree to abide by this Tender for a period of *[……..number]* days from the date fixed for tender opening of the Instructions to tenderers, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.
5. Until a formal Contract is prepared and executed, this Tender, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
6. We understand that you are not bound to accept the lowest or any tender you may receive.

Dated this _____ day of_____ 2018
[signature] [In the capacity of]

Duly authorized to sign tender for and on behalf of_____

2. PRICE SCHEDULE OF SERVICES

Please fill in the charges taking into account the scope of works in Section VI (Description of Services)

NO.	ITEM DESCRIPTION	COST
1	supply, delivery, installation, testing and commissioning of a Next-Generation Firewall for 3 years	
2	Technical training for ICT staff for 5 days	
	Total	

Signature and Stamp of tenderer _____

Please Note:-

- **In case of discrepancy between the cost per month and total, the unit cost per month shall prevail.**
- **All prices quoted shall be inclusive of all applicable taxes.**
- **Payment shall be done ones upon satisfactory supply, delivery, installation, testing and commissioning of a Next-Generation Firewall software and on submission of certified invoices and worksheets/job cards.**

3. TENDER SECURITY FORM

Whereas (name of bidder) hereinafter called <the tenderer> has submitted its bid dated (date of submission of bid) for the provision of insurance services (hereinafter called <the tender>.

KNOW ALL PEOPLE by these presents that WE (*name of bank*) of (*name of country*), having our registered office at (Name of Commission) (hereinafter called <the procuring entity> in the sum of (state the amount) for which payment will and truly to be made to the said procuring entity, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this _____ day of _____20_____

THE CONDITIONS of this obligation are:-

1. If the tenderer withdraws its tender during the period of tender validity specified by the Form: or
2. The the tender, having been notified of the acceptance of its tender by the Commission during the period of tender validity.
    (a) Fails or refuses to execute the Contract Form, if required; or
    (b) Fails or refuses to furnish the Performance security, in accordance with the Instructions to tenders.

We undertake to pay to the Commission up to the above amount upon receipt of its first written demand, without the Commission having to substantiate its demand, provided that in its demand the Commission will note the amount claimed by it is due to it, owing to the occurrence of one or both of the conditions, specifying the occurred condition(s).

This tender guarantee will remain in force up to and including thirty (30) days after the period of tender validity, and any demand in respect thereof should reach the Bank not later than the above stated date.

(**Authorized Signatories and official stamp of the Bank)**

4. MANDATORY CONFIDENTIAL BUSINESS QUESTIONNAIRE

(Must be filled by all applicants or Tenderers' who choose to participate in this tender and enclosed in the technical Bid submission envelope)

Name of Applicant(s)
……

You are requested to give the particulars in Part 1 and either Part 2 (a), 2 (b) or 2 (c), whichever applies to your type of business. Part 2 (d) to part 2(i) must be filled.
You are advised that giving wrong or false information on this Form will lead to automatic disqualification/termination of your business proposal at your cost.

Part 1 – General

Business Name:……Certificate of Incorporation / Registration No. ……Location of business premises:
Country ……..…Physical address ……
Town ……..……Building……..
Floor……Plot No. ……..……
Street / Road ……..……..……Postal Address ……..
Postal / Country Code……Telephone No's…...…
Fax No's. ……..……E-mail address ……
Website ……..
Contact Person (*Full Names*) ……Direct / Mobile No's……

Title …… Power of Attorney (**Yes / No**)
If **Yes,** attach written document.
Nature of Business (*Indicate whether manufacturer, distributor, etc)*
……..……..……..

(Applicable to Local suppliers only)
Local Authority Trading License No. …… Expiry Date ……
Value Added Tax No.……

Value of the largest single assignment you have undertaken to date (***US$/Kshs.)***
……
Was this successfully undertaken? **Yes / No**. ……(If **Yes**, attach reference)

Name (s) of your banker s)……

Branches …… Tel No's. ……

Part 2 (a) – Sole Proprietor

Full names

……

Nationality…… Country of Origin……..……

Company Profile ……

Part 2 (b) – Partnerships

Give details of partners as follows:

Full Names	**Nationality**	**Citizenship Details**	**Shares**	**Gender**
1. ……				
2. ……				
3……				
4……				

Company Profile ……(……

Part 2 (c) – Registered Company

Private or public ……

Company Profile ……

State the nominal and issued capital of the Company

Nominal KShs ……..……

Issued KShs ……..……

List of top ten (10) shareholders and distribution of shareholding in the company.

Give details of all directors as follows:-

Full Names	**Nationality**	**Citizenship Details**	**Shares**	**Gender**
1……	……	……		……
2……	……	……..		……
3……	……	……		……
4……	……	……		……..

Part 2 (d) – Debarment

I/We declare that I/We have not been debarred from any procurement process and shall not engage in any fraudulent or corrupt acts with regard to this or any other tender by the Commission and any other public or private institutions.

Full Names ……

Signature……

Dated this ……day of ……..2020.

In the capacity of ……
Duly authorized to sign Tender for and on behalf of ……

Part 2 (e) – Criminal Offence

I/We, (Name (s) of Director (s)):-

a) ……..

b) ……..……

c) ……

have not been convicted of any criminal offence relating to professional conduct or the making of false statements or misrepresentations as to its qualifications to enter into a procurement contract within a period of three (3) years preceding the commencement of procurement proceedings.

Signed ……
For and on behalf of……..……
In the capacity of ……..……
Dated this ……day of ……..2020

Suppliers' / Company's Official Rubber Stamp……

Part 2 (f) – Conflict of Interest

I/We, the undersigned state that I / We have no conflict of interest in relation to this procurement:

a) ……

b) ……

c) ……

d) ……

For and on behalf of M/s ……..
In the capacity of ……
Dated this ……day of ……2020
Suppliers' / Company's Official Rubber Stamp
……

<u>Part 2 (g) – Interest in the Firm:</u>

Is there any person/persons in the Commission or any other public institution who has interest in the Firm? Yes/No …….. (*Delete as necessary)*
Institution ……

…… ……
(Title) ***(Signature)*** ***(Date)***

Part 2(h) – Experience

Please list here below similar projects accomplished or companies / clients you have provided with similar services in the last two (2) years.

Company Name	**Country**	**Contract/ Order No.**	**Value**
1……	……	……	…….
2. ……	……	……	…….
3……	……	……	…….
4……	……	……	…….
5……	……	……	…….

Contact person (Full Names)……..
E-mail address……..
Cellphone no …… ……..

Part 2(i) – Declaration

I / We, the undersigned state and declare that the above information is correct and that I / We give the Commission authority to seek any other references concerning my / our company from whatever sources deemed relevant, e.g. Office of the Registrar of Companies, Bankers, etc.

Full names……...
Signature……
For and on behalf of M/s ……..
In the capacity of ……
Dated this ……day of ……..2020

Suppliers' / Company's Official Rubber Stamp
……

5. CONTRACT FORM

THIS AGREEMENT made the ___day of _____20____between……[name of procurement entity] of ……[country of Procurement entity](hereinafter called "the Commission ") of the one part and ……[name of tenderer] of ……[city and country of tenderer](hereinafter called "the tenderer") of the other part.
WHEREAS the Commission invited tenders for certain materials and spares. Viz……..[brief description of materials and spares] and has accepted a tender by the tenderer for the supply of those materials and spares in the spares in the sum of ……[contract price in words and figures]

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

    (a) the Tender Form and the Price Schedule submitted by the tenderer;
    (b) the Schedule of Requirements;
    (c) Description of the services to be performed
    (d) the Technical Specifications;
    (e) the General Conditions of Contract;
    (f) the Special Conditions of Contract; and
    (g) The Commission's Notification of award.

3. In consideration of the payments to be made by the Commission to the tenderer as hereinafter mentioned, the tenderer hereby covenants with the Commission to provide the materials and spares and to remedy defects therein in conformity in all respects with the provisions of the Contract.
4. The Commission hereby covenants to pay the tenderer in consideration of the provision of the materials and spares and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, sealed, delivered by_____the _____(for the Commission)

Signed, sealed, delivered by_____the _____(for the tenderer)
in the presence of_____.

6. PERFORMANCE SECURITY FORM

To: ……..
[name of the Commission]

WHEREAS……[name of tenderer]
(hereinafter called "the tenderer") has undertaken, in pursuance of Contract No._____[reference number of the contract] dated _____20_____to
supply……..
[Description services](Hereinafter called "the contract")
AND WHEREAS it bas been stipulated by you in the said Contract that the tenderer shall furnish you with *a* bank guarantee by a reputable bank for the sum specified therein as security for compliance with the Tenderer's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the tenderer a guarantee:
THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the tenderer, up to a total of ……
[amount of the guarantee in words and figures],
and we undertake to pay you, upon your first written demand declaring the tenderer to be in default under the Contract and without cavil or argument, any sum or sums within the limits of ……..
[amount of guarantee] as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.
This guarantee is valid until the _____ day of 20 _____
Signature and seal of the Guarantors

_____
[name of bank or financial institution]

_____
[address]

_____
[date]

(Amend accordingly if provided by Insurance Company)

APPENDIX A: SAMPLE LETTER OF NOTIFICATION OF AWARD

REPUBLIC OF KENYA

PARLIAMENT OF KENYA

M/S
P. O. Box
Nairobi

Dear Sir/Madam,

RE: SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF A NEXT-GENERATION FIREWALL (TENDER NO. PJS/017/2019-2020)

Your Bid dated …….. amounting to Kenya Shillings …… only for Supply, Delivery, Installation, Testing, Training and Commissioning of a Next-Generation Firewall is hereby accepted.

The Contract Documents are in the course of preparation and you will be called to sign them after seven (7No.) days have elapsed from the date of this letter.

The duration of this contract will be for three years from the date of commencement renewable for a further period subject to satisfactory performance and the payment will be as per the Contract.

The …… is hereby appointed Contract Manager in connection with your contract for the provision of the above services.

Please acknowledge your acceptance of the offer within seven (7) days from the date of this letter and communicate with the Contract Manager immediately and thereafter on all matters relating to the contract.

Yours faithfully,

DIRECTOR GENERAL, PARLIAMENTARY JOINT SEERVICES
PARLIAMENTARY SERVICE COMMISSION