SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

T# 01/19-20

Invitation to Bid

The Securities & Exchange Commission of Pakistan invites sealed bids from the services providers, principal's authorized dealers/distributors/partners/resellers based in Pakistan and registered with Federal Board of Revenue/Respective Revenue Boards for Income Tax and Sales Tax and who are on Active Taxpayers List (Income and Sales tax) of the Federal Board of Revenue/Relevant Tax Authority for following requirements

S. No.	Requirements	Tender Ref No.
1	Web Application Firewall (Reverse Proxy)	T# 01 (i)/19-20
2	Wireless Access Points (WAPs) for SECP Head Office, Islamabad, Lahore and Karachi offices.	T# 01 (ii)/19-20
3	Acquisition and Development of a Chatbot	T# 01 (iii)/19-20

Bidding documents containing detailed terms and conditions, method of procurement, procedure for submission of bids, bid bond/security, bid validity, opening of bid, evaluation criteria, clarification/rejection of bids etc. against above requirement are available for the interested bidders from the undersigned and can also be downloaded from https://www.secp.gov.pk/procurement/

The bids prepared in accordance with the instructions in the bidding documents, must reach undersigned on or before Sept 16, 2019 by 1500 Hrs and will be opened on the same day at 1530Hrs.

In case of any query, Admin Department may be contacted on Telephone No. 051-9207091-4 (Ext-437) during office hours (Monday to Friday excluding Public Holidays)

Deputy Director (Admin)

Terms and Conditions for Bids and Bidders

1. **Tender Identification Number: TENDER # 01 (i)/19-20**

2. **The Procurement Agency is:**

Securities and Exchange Commission of Pakistan
4th Floor, NICL Building, 63 Jinnah Avenue, Blue Area,
Islamabad.

3. The Securities and Exchange Commission of Pakistan invites sealed bids from the service provider based in Pakistan and registered with Federal Board of Revenue/Respective Revenue Boards for Income Tax and Sales Tax and who are on Active Taxpayers List (Income and Sales tax) of the Federal Board of Revenue/Relevant Tax Authority for

PURCHASE OF WEB APPLICATION FIREWALL (REVERSE PROXY)

through

SINGLE STAGE TWO ENVELOP METHOD.

4. Bid shall comprise a single package containing TWO separate envelopes. Each envelope shall contain separately the financial Bid and the technical Bid. The envelopes shall be clearly marked as **"FINANCIAL BID"** and **"TECHNICAL BID"** in bold and legible letters.

5. The Bid Bond to be enclosed in a **SEPARATE ENVELOPE**, labelled as **"BID BOND",** and should be **SEALED** and enclosed in the main envelop.

6. BID Bond should not be ENCLOSED in the envelope of financial OR technical proposal.

7. Initially, only the envelope marked **"TECHNICAL BID"** shall be opened publicly. The envelope marked as **"FINANCIAL BID"** shall be retained.

8. After the evaluation and approval of the technical bid, financial bids of the technically accepted bids only will be opened at a time, date and venue announced and communicated to the bidders in advance. Financial bids of technically unsuccessful bidders will be returned.

9. The amount of the bid and bid bond/security shall be in Pak rupees. The bids should be accompanied by bid bond/security (refundable) for an amount equal to 2% of the total quoted price (inclusive GST, if applicable) in shape of either pay order, demand draft valid for not less than 6 months in favor of Securities and Exchange Commission of Pakistan.

10. Bids not accompanied by bid bond/security or with less amount of bid bond/security will not be entertained.

11. In case any bidder submits more than one option against this invitation then bid bond/security shall be submitted against highest quoted option.

12. Only registered suppliers who are on Active Taxpayers List (ATL) of FBR are eligible to supply goods/services to the Commission.

13. If any supplier is not in ATL at the time of payment then his payment shall be stopped till he files his mandatory returns and appears on ATL of FBR.

14. Tax shall be deducted/withheld as per applicable sales tax and income tax law.

15. Relevant details plus terms and conditions of the invitation may be obtained from the undersigned personally or by visiting the SECP website: https://www.secp.gov.pk/procurement/

16. SECP reserves the right to cancel this invitation and reject all bids at any stage of the bidding process.

17. The bid validity period shall be 150 days.

18. If the bid is withdrawn after bid opening time and before the expiry of bid validity the bid bond/security will be forfeited in favor of the SECP, Islamabad.

19. The language of the bid is English and alternative bids shall not be considered.

20. Amendments or alterations/cutting etc., in the bids must be attested in full by the person who has signed the bids.

21. The prices quoted shall correspond to 100% of the requirements specified. The prices quoted by the bidder shall not be adjustable. Changes or revisions in rates after the opening of the bids will not be entertained and may disqualify the original offer.

22. The rates must be quoted strictly in accordance with our documents and Annex(s).

23. Discounts (if any) offered by the bidder shall be part of the bid and for taxation purposes will be treated in accordance with the applicable laws.

24. Detail of applicable taxes and whether taxes included or not in the quoted price and breakup of the quoted price shall be clearly mentioned.

25. The bidder shall be responsible for payment of any duties/taxes etc. which are imposed by the Government of Pakistan (GOP). The bided price MUST be inclusive of all applicable taxes. The bidder is hereby informed that the Commission shall deduct tax at the rate prescribed under the tax laws of Pakistan from all payments for supply/services rendered by any responding organization who accepts the Purchase order or signs agreement with the Commission.

26. In case applicable taxes have neither been included in the quoted price nor mentioned whether quoted amount is inclusive or exclusive of such taxes, then

27. Quoted amount will be considered inclusive of all taxes.

28. Selected service provider will have to provide the required services/equipment, if selected and declared as best evaluated bidder. In case selected bidder is not willing to supply on quoted amount then bid bond/security submitted with the bid will be forfeited in favor of the Commission.

29. Bidder must have regular place of business, telephone numbers and email address and must provide proof of their existence in the particular business. A brief profile of the bidder, along with list of major customers (corporate sector) along with their contact details is required.

30. Items included in Compulsory Certification Scheme of PSQCA shall be duly certified by an accredited laboratory and fulfill necessary conditions of PSQCA, as applicable.

31. Bidder must submit following undertakings (on stamp paper of Rs. 100):

    a. Affidavit that the documents/details/information submitted is true and liable to be rejected i f proven false and in that case legal action is liable on that bidder.

    b. Affidavit that the bidder has never been blacklisted by any Government / Semi Government/ Autonomous organization

32. Comprehensive warranty & onsite support for mentioned years shall be given for the

equipment/software/renewal at Islamabad, Karachi, and Lahore offices (if applicable).

33. All software based items contains installation and configuration and end user orientation which is responsibility of the supplier (if support is not provided by the Principal).

34. The equipment/software/renewals supplied must be duty paid in respect of all applied duties and taxes.

35. The quantities required may increase/decrease according to SECP requirement.

36. The end user License, end user warranties and end user support services will be in the name of SECP for all equipment and software loaded on the equipment delivered.

37. A copy of valid authorized agency/partnership/dealership/distributorship certificate from their principals is to be submitted with the bid in case of any such claim.

38. Payment shall be made after delivery, installation and commissioning of complete equipment/licenses/services/renewals. All payments shall be made after deduction of taxes and all payments shall be made through cross cheque in Pak Rupees. Taxes will be deducted at source as per Government Rules at the time of payment.

39. The bidders do not have the option of submitting their bids electronically. Telegraphic and conditional bids will not be accepted.

40. Unsealed bids will not be accepted.

41. **Sealed bids may be dropped in the tender drop box placed at Ground Floor of the NIC Building, 63 Jinnah Avenue, Islamabad.**

42. Clarification if any on the requirements may be obtained from:
    - asim.ayaz@secp.gov.pk

43. The bid bond/security of successful bidder will be retained and returned after delivery, installation and commissioning of complete equipment/licenses/services/renewals of ordered items. However, bid bond/security of unsuccessful bidders will be returned after award of contract to successful bidder.

44. Bid security of successful bidder will be released after submission of Performance Guarantee i.e. Pay order/Demand draft, equivalent to 10% of the value of Contract/Purchase Order. The Performance Guarantee will be released after successful completion of the warranty period and verification/confirmation by IT Dept.

45. During the retention period the bid bond/security, money can be utilized by Commission. Moreover, no interest / markup will be provided on this amount by Commission to bidder at the time of refund/release of bid bond/security.

46. Successful bidders shall be bound to provide the required items within the delivery period. In case of late delivery, late delivery (LD) charges equivalent to 1% (of the PO/contract Value) per week shall be imposed and deducted from the payment. However, imposed penalty shall not exceed 10% of the PO/contract value.

47. In case 1st lowest bidder is unable to supply ordered items then the Commission reserve the right to award the contract to 2nd lowest evaluated bidder. In case 2nd lowest evaluated bidder is unable to supply ordered items then the Commission reserve the right to award the contract to 3rd lowest evaluated bidder.

48. Bid bond/security of the bidder who is unable to supply ordered items shall be forfeited in favor of

the Commission.

49. The Commission reserves the right either to issue a Purchase Order or sign an agreement with the successful bidder OR PO & Agreement both will be executed.

50. The bids received after the due date and time will not be entertained.

51. It is of utmost importance that bids should be submitted very carefully and the instructions set forth above, scrupulously complied with, failing which the offer will be ignored.

52. The place of bid destination is:

Securities and Exchange Commission of Pakistan,
NICL Building, 63 Jinnah Avenue, Blue Area, Islamabad.

53. The envelopes shall bear the following additional identification marks:

Bid for:	**PURCHASE OF WEB APPLICATION FIREWALL (REVERSE PROXY)**
Bidder Name:	XYZ
Attention:	M. Ubaidullah Khalid, Deputy Director, Admin, 4th Floor, NICL Building, 63 Jinnah Avenue Blue Area, Islamabad

54. The deadline for the submission of bids is:
Date: September 16, 2019
Time: 1500Hrs

55. The bid opening shall take place at

Securities and Exchange Commission of Pakistan NICL Building, 63 Jinnah Avenue, Blue Area, Islamabad

Date: September 16, 2019
Time: 1530Hrs

A statement "Not to be opened before 1530 Hrs on September 16, 2019" shall be clearly mentioned on the top of the sealed bid.

Note: Attachment Details are as under:

1.	**Terms of Reference/Technical Specifications**	**Annex "A"**
2.	**Evaluation Criteria**	**Annex "B"**
3.	**Format for Financial Bid**	**Annex "C"**

If the above terms and conditions are acceptable then bids must be submitted well in time and according to the requirements.

Annex – "A"

TERMS OF REFERENCE	
Requirement	**Quantity**
Web Application Firewall (Reverse Proxy)	01
Delivery Information	
The firewall must be delivered and installed at SECP Head Office, Islamabad	
Data Center Web Application Firewall (Reverse Proxy)	
Web Application Firewall must be of data center class providing filtered traffic to and from hosted web applications with reverse proxy capabilities	
Web Application Firewall Performance Requirements	
Web Application Firewall throughput	500 Mbps or higher
Hypervisor Support	VMware and other hypervisors
High availability Support	Active-Active and Active-Standby
vCPU	04 or more
Memory Support	04 GB or higher

Table 1: Web Application Firewall Performance Requirements

S. No.	Feature Requirements
1.	The proposed solution MUST be a virtual appliance
2.	The proposed solution MUST inspect HTTP, HTTPs, & FTP to prevent attacks
3.	The proposed solution MUST provide Protection against OWASP Top Ten security risks
4.	The proposed solution MUST be PCI/ DSS compliant
5.	The proposed solution MUST support SSL/ TLS offloading
6.	The proposed solution MUST prevent access by unauthorized IP(s) and subnets
7.	The proposed solution should have a database of signatures, designed to detect known problems and attacks
8.	The proposed solution MUST Support automatic updates to the signature database, ensuring complete protection against the latest application threats.
9.	The proposed solution should have ability to correlate multiple security events together to accurately distinguish between good and bad traffic
10.	The proposed solution MUST support custom security rules, Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria
11.	The proposed solution should have Reputational Base Service which can provide a near-real time live feed of the following known attack sources: •Malicious IPs •Botnets •Phishing URLs •Anonymous Proxies •Spams
12.	The proposed solution should have "anti-automation" protection, which can block the automated attacks using hacking tools, scripts, framework etc.
13.	The proposed solution MUST Inspect and monitor all HTTP(s) data and the application levels including HTTP headers, form fields, and the HTTP body
14.	The proposed solution should support reporting and logging facilities

15.	The proposed solution should be able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution
16.	The proposed solution should support SNMP v1/v2c & v3
17.	The proposed solution should provide customized logging levels and filters
18.	The proposed solution should provide reports based on PCI Compliance, Attack Activities, Traffic Activities, Event Activities in multiple formats like, HTML, PDF, MS-Word, Text & MHT with the capability of sending these reports to Email/Group of Email Addresses and FTP Server
19.	The proposed solution should provide high-level dashboard of system status and Web activity
20.	The proposed solution should have the ability to integrate with standard Security Event Management tools / system
21.	The reporting information should contain at least the following information: •Source to Destination connection information •Extensive packet header information •Raw and Hex body presentation for POST parameters •Signature match in preventing the attack •Pattern Match Log should be able to provide top attacks, top source and countries of attacks in GUI
22.	The proposed solution should have a Data-analytics dashboard
23.	The proposed solution should have Botnet Analysis information dashboard
24.	The proposed solution should have Blocked IPs information dashboard
25.	The proposed solution should have Client device management information dashboard
26.	The proposed solution must have the functionality to release the blocked IP addresses
27.	The proposed solution MUST support on-board Anti-Virus without any additional software/hardware/third-party Anti-Virus solution
28.	The solution must support following deployment modes •Reverse Proxy •Offline Protection •Transparent Proxy/Inspection
29.	The proposed solution should support protection from Network and Application Level DoS
30.	The proposed solution should support multiple Certificates to be imported which can be used for different published websites
31.	The proposed solution should support Web-Anti-Defacement
32.	The proposed solution should support load balancing based on Round-Robin, Weighted Round-Robin, Least Connection, URI/Full URI Hash, Host Hash, Host Domain Hash & Domain Hash
33.	The proposed solution should be capable of supporting persistency features like Persistent IP, Persistent Cookies, Insert Cookies
34.	The proposed solution should support Content routing for HTTP
35.	The proposed solution should support X-Forwarder & CAPTCHA
36.	The proposed solution should be able to provide Caching and Compression Solution
37.	The proposed solution should provide an ability to administrator to create custom attack signature, other than pre-defined known signatures
38.	The proposed solution should support user scoring based on its activity on a session. This scoring should be used to deny the connection
39.	The proposed solution should support Automatic learning/profiling of the activity happening on the published services
40.	The proposed solution should support URL Rewriting, and Layer-7 Server Load Balancing
41.	The proposed solution should support behavioral validation to prevent from unknown application attacks
43.	The proposed solution should support on-box AV scanning for uploaded files

44.	The proposed solution should have the ability to detect attacks at multiple levels, including operating system, Web server software and application-level attacks: • XML and JSON protocol conformance, • Malware Detection, • Protocol Validation, • Brute Force Protection, • Cookie Signing and Encryption, • Syntax-based SQLi detection, • HTTP Header Security, • Custom error message and error code handling, • Data leak prevention, • Web-Sockets support, • Cross site scripting (XSS), • Layer 4 & Layer 7 DoS and DDoS, • Generic Attacks, • Trojans, • Known Exploits, • Information Disclosure, • Form Field Parameter Tampering and HPP tampering, • Session hijacking, • Cookie manipulation and poisoning, • Buffer Overflows, • Credit Card Detection, • Protection against known database and Web server vulnerabilities, • Forceful browsing, and • Broken access control
Administration and Authentication	
45.	The proposed solution should support web-based and CLI-based access methods
46.	The proposed solution should support role-based access control
Vulnerability Assessment and Management	
47.	The proposed solution should provide a Vulnerability Assessment and provide a detailed Assessment Report for the monitored WEB Application(s)
48.	The proposed solution should have the ability to measure compliance with industry standards and regulations
49.	The proposed solution should natively support HTTP2 as well as HTTP1.x
50.	The proposed solution should support Virtual Patching for the backend servers
51.	Product roadmap: • The roadmap of the quoted product must be shared • The quoted product must not have an announced end of marketing/ sale date • The quoted product must remain in support by the Principal for at least next 05 years

Table 2: Web Application Firewall Feature Requirements

Annex – "B"

Technical Evaluation Criteria

Sr. No.	Description	Marks
1.	05 years comprehensive warranty with 24x7 technical support from the Principal	**MUST**
2.	Valid Partnership Letter with Principal/ Manufacturer	**MUST**
3.	Authorization Letter from Principal for Tender Participation	**MUST**
4.	Bidder must have history of similar projects of IT security solution deployments of minimum 05 years (attach POs as proof)	**MUST**
5.	Bidder shall provide details of Technical resources and project team (share resumes)	**MUST**
6.	Product roadmap: • The roadmap of the quoted product must be shared • The quoted product must not have an announced end of marketing/ sale date • The quoted product must remain in support by the Principal for at least next 05 years	**MUST**
7.	The quoted solution should provide comprehensive reporting and alerts for both general and focused information	**MUST**
8.	Antivirus, IP reputation, Protocol validation, Attack Signatures Updates, Unknown Application attacks for a period of 05 years subscription	**MUST**
9.	Gartner 2018 Magic Quadrant for Web Application Firewalls (Leaders & Challengers Only)	**MUST**
10.	Performance requirements (as in Table-1) and Feature requirements (as in Table-2) of the above TOR	**MUST**
11.	Free of cost professional hands on training for 02 SECP resources	**MUST**
12.	Deployment, installation and configuration shall be vendor's responsibility	**MUST**
13	Vendor must have geographical presence at Islamabad, Lahore and Karachi	**MUST**

Table 3: Technical Evaluation Criteria

NOTE:

1. The bidders MUST submit a compliance sheet against mentioned performance requirements, feature requirements, and the technical evaluation criteria.
2. Bids NOT in compliance with MUST items in the evaluation criteria will NOT be evaluated.

FORMAT FOR COMPLIANCE SHEET

SR	ATTRIBUTE	SPECIFICATION	COMPLIANCE (YES/NO/PARTIAL)

Annex – "C"

FORMAT FOR FINANCIAL BID ONLY

S#	Quoted Item (Brand, Model etc.)	Unit Price with all applicable taxes	Total Price with all applicable taxes
1.			