SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

T# 21/19-20

Invitation to Bid

The Securities & Exchange Commission of Pakistan invites sealed bids from the service providers 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

Vulnerability Assessment and Penetration Testing (VAPT)

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 free of cost 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 **January 13, 2020** by 1030Hrs and will be opened on the same day at 1100Hrs.

In case of any query, Admin Department may be contacted on Telephone No. 051-9207091-4 (Ext-437/444) during office hours (Monday to Friday excluding Public Holidays)

Deputy Director (Admin)
NICL Building, 63 Jinnah Avenue, Blue Area Islamabad

Terms and Conditions for Bids and Bidders

1. Tender Identification Number: **TENDER # 21/19-20**

The Procurement Agency is:

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

2. The Securities and Exchange Commission of Pakistan invites sealed bids from service providers 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

Vulnerability Assessment and Penetration Testing (VAPT)

through

SINGLE STAGE TWO ENVELOP METHOD

3. 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.

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

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

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

7. 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.

8. 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.

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

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

11. Only registered suppliers who are on Active Taxpayers List (ATL) of FBR are eligible to supply goods/services to the Commission. **Bids of all those bidders not found on ATL shall be rejected.**

12. 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.

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

14. 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/

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

16. The bid validity period shall be 150 days.

17. 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.

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

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

20. 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.

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

22. 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.

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

24. 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.

25. 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 quoted amount will be considered inclusive of all taxes.

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

28. 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 (email/ mobile number) is required.

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

30. Bidder must submit following on stamp paper of Rs.100, **failing which the bid shall be rejected:**

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

    b) Affidavit that the bidder has never been blacklisted by any National/International organizations.

31. Comprehensive warranty & onsite support for mentioned years shall be given for the equipment/software/renewal at Islamabad, Karachi, and Lahore offices (if applicable).

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

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

34. The quantities may increase/decrease according to SECP requirement.

35. 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.

36. A copy of valid authorized agency/partnership/dealership/distributorship certificate from their principals is to be submitted with the bid. (if applicable)

37. 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.

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

39. Only sealed bids will be accepted/opened and unsealed bids will be rejected.

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

41. Clarification if any on the requirements may be obtained from: ubaidullah.khalid@secp.gov.pk

42. 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/services. However, bid bond/security of unsuccessful bidders will be returned after award of contract to successful bidder.

43. During the retention period the bid bond/security no interest / markup will be provided on this amount by Commission to bidder at the time of refund/release of bid bond/security.

44. Successful bidders shall be bound to provide the required items/services 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.

45. In case 1st lowest bidder is unable to supply ordered items/services 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/services then the Commission reserve the right to award the contract to 3rd lowest evaluated bidder.

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

47. 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.

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

49. 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.

50. Bids received will be evaluated as per evaluation criteria given in the TORs.

51. The place of bid destination is:

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

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

Bid for:	**Vulnerability Assessment and Penetration Testing (VAPT)**
Bidder Name:	XYZ
Attention:	M. Ubaidullah Khalid, Deputy Director (Admin) 4th Floor, NICL Building, 63 Jinnah Avenue Blue Area, Islamabad

53. The deadline for the submission of bids is:

Date:	January 13, 2020
Time:	1030Hrs

54. The bid opening shall take place at
Securities and Exchange Commission of Pakistan
NICL Building, 63 Jinnah Avenue, Blue Area, Islamabad
Date: January 13, 2020
Time: 1100Hrs

55. A statement “Not to be opened before 1100 Hrs. on January 13, 2020” shall be clearly mentioned on the top of the sealed bid.

Note: Attachment Details are as under:

- Scope of Work **Annex “A”**
- Technical Evaluation Criteria **Annex “B”**
- Documentary Evidence **Annex “C”**
- Sample Agreement **Annex “D”**
- Sample Non- Disclosure Agreement **Annex “E”**

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

Annex – "A"

Vulnerability Assessment and Penetration Testing (VAPT)

Scope of Work (SOW)

The bidders are requested to conduct vulnerability assessment and penetration testing (VAPT) to determine security weaknesses and vulnerabilities in Commission's IT infrastructure, applications, databases and web applications. The bidder should have proven track record in Information Security domain and have extensive experience of VAPT testing for both, public and private sector organziations. Four tests are to be conducted by the vendor, with following details:

1. **Black Box:** No prior information will be given to service provider except the target IP Addresses.
2. **Grey Box:** Limited information of target system e.g. IP address, application URLs and frontend etc. would be provided. Authentication credentials will not be part of provided information.
3. **White Box:** Services authentication credentials will be provided in addition to the information that was provided in the Grey Box testing.
4. **Follow-up:** After the submission of above-mentioned testing (Black box, Grey box, and White box) reports, SECP will discuss and implement the security fixes recommended by the vendor in the reports. The service provider will be required to verify these measures by performing associated vulnerabilities testing.

The details of IPs (Private and Public) will be shared after the award of contract. Total number of public IPs to be tested will be upto twenty five (25). Non-disclosure agreement (NDA) will be signed with selected bidder before sharing any information.

Target Identification and Analysis Techniques:

Technical target identification and analysis techniques are required to focus on identifying active devices and their associated ports and services, and analyze them for potential vulnerabilities. This includes but not limited to the below mentioned targets and techniques.

- Systematic and thorough identification of information assets (data, information systems, information processing facilities)
- Security architecture and configuration review of critical assets (Servers, Storage, OS, and DB etc.)
- Physical assessment of technical infrastructure
- Identification of potential risks to the identified information assets
- Evaluation of existing security measures and their effectiveness
- Network Discovery
- Network Port and Service Identification
- Firewall diagnostics
- VPN and remote infrastructure
- DMZ security
- Directory services and Messaging infrastructure

- Vulnerability Scanning

    - Check compliance with host application usage and security recommendations
    - Provide information on targets for penetration testing
    - Provide information on how to mitigate discovered vulnerabilities
- Wireless Scanning
    - Passive Wireless network Scanning
    - Active Wireless network Scanning
- Website/ Web-Application assessment should include but not limited to below assessment techniques:
    - Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF)
    - Vulnerabilities to SQL/ HTTP/ CRLF/ IFrame Injections
    - Directory Traversal
    - Authentication hacking/ attacks
    - Password strength on authentication pages
    - File inclusion attacks
    - Web server information security
    - Phishing a website
    - Buffer Overflows and Invalid Inputs
    - Malicious File Execution
    - Insecure Direct Object Reference
    - Information Leakage and Improper Error Handling
    - Broken Authentication and Session Management
    - Insecure Communications
    - Failure to Restrict URL Access etc.

Target Vulnerability Validation Techniques:

The objective is to prove that a vulnerability exists, and to demonstrate the security exposures that occur when it is exploited. Few of the below vulnerabilities assessment techniques are listed below:

- Password cracking and spraying for all internal/external applications
- Exploiting Microsoft Exchange Server
    - Get Global address list
    - Testing OWA/ EWS/ MAPI/ ActiveSync etc.
- Social Engineering

Assessor Selection and Skills:

The Assessors testing methodology should not only include results of thorough testing of the entire target environment, but should also include a detailed report in deliverables with both tactical and strategic recommendations. These recommendations should be both actionable and advisory in nature, and should correlate to organization's business goals.

The VAPT should be based on the most widely used industry standards for security testing namely:

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information System Security Assessment Framework (ISSAF)
- LPT (Licensed Penetration Tester) methodology from EC-Council
- WASC-TC (Web Application Security Consortium Threat Classification)
- PTF (Penetration Testing Framework)
- NIST SP800-115 (Technical Guide to Information Security Testing and Assessment)

The penetration testing approach and risk assessment methodology should be compatible with globally known compliance standards and regulations.
The Assessors should have certified and trained people in multiple domains to perform the said testing. Some of them are mentioned below:

- Expertise in network security, breaching firewalls and intrusion detection/ prevention systems
- Complete operating system knowledge both of client and server
- In depth knowledge of web based technologies/ applications

Assessor's Responsibilities:

- Provide resources with desired expertise and resource charting (time each resource will dedicate on each phase of the project)
- Devise and share methodology for identification of information assets
- Share details of all the tools to be used for VAPT
- Proposed schedule for completing the requirements mentioned in the RFP including testing window for production website and applications
- Informing the appropriate stakeholders—such as security officers, management, system administrators, and users—of security assessment activities
- Developing assessment plans with relevant system/ security managers and the CISO

- Executing examinations and tests, and collecting all relevant data as per SOW
- Analyzing collected data and developing mitigation recommendations
- Conducting additional examinations and tests for validating the mitigation actions
- **Submission of assessment reports**
  - Review of the current security state of SECP IT infrastructure/ information assets
  - A list of deficiencies tied to the system/ process for focused remediation for both internal and external testing
  - VAPT report including threats and vulnerabilities to SECP's information assets including probability and impact using/referring industry standards and best practices
  - Detailed recommended remediation measures for each identified threat, vulnerability and deficiency
  - If suggested recommendations for risk mitigation/ removal could not be implemented; alternate solutions to be provided
  - An executive report for senior management should also be submitted summarizing the approach, findings, and recommendations
  - Presentation for the senior management
  - A security roadmap for the Commission to ensure compliance and address the security gaps including investments to reinforce IT security
  - Final consolidated report after follow up testing of the entire environment

Project Timelines:

- The black box, grey box, and white box testing MUST be completed within 60 calendar days after the award of contract
- SECP will implement the recommended security fixes within 60 days of receiving the report

- Followup testing by the bidder MUST be completed within 30 days of SECP go ahead

Project Team:

- The bidder must share complete details of project team along with their roles in the project and detailed CVs
- The project team must include a project manager, who will be the POC from the bidder side
- SECP will appoint a project manager/ POC for the VAPT project

Payment Terms

- 50% after completion of black box, grey box, and white box testing and submission of report for these.
- Remaining 50% after successful completion/ closure of the whole VAPT exercise/ project i.e., after the follow-up testing is done.

Annex – "B"

Technical Evaluation Criteria

S. No.	Description	Marks
1.	Complete compliance with SOW including assessor's responsibilities and project timelines, project team etc.	**MUST**
2.	The service provider must have performed similar testing in public sector. Work order proofs as well as satisfactory completion certificates from at least 05 references (at least 02 public sector organizations) of a size comparable to or greater than SECP, attach proofs with contact details of references. The decision will be made after obtaining feedback from references.	**MUST**
3.	The service provider must have at least three (03) certified hackers/penetration testers or certified information security auditors (CISA) on board and must have minimum of 05 years' experience in Information Security domain, attach proofs.	**MUST**
4.	The bidder must have carried out at least three (03) penetration testing projects in last three (03) years, attach proofs.	**MUST**
5.	The bidders **MUST** submit a technical compliance sheet (given format) against all requirements mentioned in the technical evaluation criteria.	**MUST**
6.	VAPT professional hands on training for at least two SECP resources using relevant tools.	**MUST**

NOTE:

1. Bids **NOT** in compliance with **MUST** items in the evaluation criteria will **NOT** be evaluated.

FORMAT FOR TECHNICAL COMPIANCE SHEET

SR	SPECIFICATION	COMPLIANCE (YES/NO/ PARTIAL)	COMPLIANCE PROOF (PAGE NUMBER IN BID)

Financial Evaluation

- Bids in compliance with **Must** requirements in the technical evaluation criteria and quoting lowest cost shall be selected.

Annex – "C"

DOCUMENTARY EVIDENCE

Name of the Bidder: _____

Bid against Reference No: _____

Date of opening of Bid: _____

Documentary evidence for determining eligibility of the bidders & evaluation of bids. Bidders should only initial against those requirements that they are attaching with the form. Bidders are required to mention the exact page number of relevant documents placed in the Bid. Bidders are advised to attach all supporting documents with this form in the order of the requirement.

S #	Required Documentation	Signature of Bidder	Supporting Document's Name	Page Number in the Bid.
1	NTN Certificate			
2	GST Certificate			
3	Availability on Active Tax Payers List of FBR			
4	Registration/Incorporation/Business Certificate			
5	Affidavits			
6	Bid Bond/Security (As applicable)			
7	Bid Validity period of 150 days (As applicable)			
8	Original Bidding documents duly signed/ stamped			

Annex – "D"

SAMPLE AGREEMENT

This agreement ("Agreement") is made on this_____ day of _____ 2020,

By and Between

Securities & Exchange Commission of Pakistan, a statutory body established in pursuance of the Securities and Exchange Commission of Pakistan Act, 1997 ("SECP Act 1997"), having its Head Office at NICL Building, 63-E, Jinnah Avenue, Islamabad, Pakistan (hereinafter referred to as the **"Commission"** which expression shall be deemed to include, where the context so permits, its successors in interests, administrators and permitted assigns) OF THE ONE PART;

And

XYZ (Pvt.) Limited having its registered **Office Address**, Pakistan (herein after referred to as the **"Contractor"** which expression shall be deemed to include, where the context so permits, its successors in interests, administrators and permitted assigns) OF THE OTHER PART;

The Commission and the Contractor may hereinafter individually be referred to as Party and collectively as Parties.

WHEREAS:

A- The Commission requires Vulnerability Assessment and Penetration Testing (VAPT) services ("Services") from a competent firm dealing in Security Assessment services for shared requirement at its Head Office Islamabad.

B- The Contractor represents and warrants that it has the requisite expertise and resources to provide the services required by the Commission.

C- The Contractor has agreed and the Commission has approved the Services to be provided by the Contractor on the terms and conditions mentioned herein below.

Now, therefore, in consideration of the mutual covenants and agreements herein contained, the parties hereto, intending to be legally bound, agree as follows:

1-Duration

1-1. This Agreement will become effective as of _____ and will remain in effect for a period of **Six Months** (the "Term"). The termination of this Agreement will not:

(a) relieve either party from any expense, liability or obligation or any remedy therefore which has accrued or attached prior to the date of such termination, nor.

(b) cause either party to lose, surrender or forfeit any rights or benefits which have accrued at the time of termination.

1-2. Prior to the expiration of the term, this Agreement may be extended for a further period by mutual agreement between the parties, provided that, the parties must enter in to a mutual written agreement to extend the term. When used in this agreement, the phrase "the Term" shall refer to the entire duration of the Agreement.

2-Scope of Work

2-1. The Services to be provided by the contractor under this Agreement shall be in accordance with Schedule-A.

3- Payments

3-1. The Contractor will charge the Commission a fixed amount of PKR XXX (inclusive of all taxes) for Vulnerability Assessment and Penetration Testing of External and Internal SECP Networks. The payment will be 50% after completion of black box, grey box, and white box testing and submission of report and remaining 50% after successful completion/ closure of the whole VAPT exercise/ project and signoff.

3-2. If SECP is not able to complete the patches within six (06) months after submitting VAPT report, remaining 50% of the payment at signoff should be released without any delay.

3-3. After applying all the patches after the first report, the Contractor will conduct follow up testing and share the report with the Commission along with presentation(s) to senior management. This will close the contract and in case of any additional follow up test needs, any re-testing activity will be considered beyond the scope of the contract.

3-4. The Commission will ensure timely payments within forty-five (45) days of the receipt of an invoice from the Contractor.

3-5. Any payments made under this Agreement by the Commission shall be less any Government taxes, which the Commission is authorized under the law to deduct.

4-Contractor Obligations

4-1. The Contractor will engage its own employees / staff at the premises and employees / staff shall be qualified to perform Security Assessment and penetration Testing.

4-2. The Contractor will be exclusively responsible for all legal benefits to its staff / employees including compensation for death, injury etc. while performing the Contractor's obligations under this Agreement and the Commission shall have no obligation or responsibility on any account whatsoever.

4-3. The Contractor shall be responsible for all acts or omissions of any of its staff or personnel working on the Commission's premises and shall be liable for any loss or damage suffered by the Commission and shall compensate the Commission accordingly.

4-4. The Contractor will indemnify the Commission against all the damages or losses etc. that may be caused by his staff / employees due to any reason whatsoever, including but not limited to theft, malignance and pilferage etc.

4-5. The work done and standards observed / maintained by the Contractor will be checked, inspected and reviewed by the authorized officer(s) of the Commission to ensure that the work is being done and standards are observed as per terms of the Agreement and agreed specification, who may issue or give such notice, advises or reminders to the Contractor as may be necessary for the proper execution of the Agreement.

4-6. The authorized officers of the Commission will at all the time have free access to all part of the work area where the work carried out by the Contractor is in progress. The Contractor will extend all possible help and facilitate as may be required by Commission.

4-7. The billing invoice of the Contractor will be verified by authorized officer(s) of the Commission to check whether the Contractor has fulfilled his obligations as per terms of the Agreement and the payment will be made to the contractor accordingly.

4-8. The Contractor shall ensure that it obtains the necessary insurance coverage for its staff employees deputed at the premises for any loss or damage.

5- Termination

5-1. This Agreement may be terminated by either party by providing thirty (30) days prior written notice to the other party if the other party is in material breach of its obligations under this Agreement and the breach has not been remedied for a period of fifteen (15) days after the notice has been issued.

6- Dispute Resolution

If any dispute arises at any time between the parties:

6-1. The parties shall endeavor to resolve such differences amicably.

6-2. In the event of that such differences cannot be resolved within a period of fifteen (15) days: the matter shall be referred to the Departmental Head IT of the Commission, whose decision shall be final and binding on both the parties.

7- Force Majeure

7-1. Any failure or omission by any party to perform any obligation under this Agreement shall not be deemed a breach to the extent that such failure or omission is caused by any supervening event (event of the force majeure) beyond the reasonable control of party so effected (to include but not limited to acts of God, acts of Government, war explosions, terrorism, sabotage, natural disaster, riots, civil commotion, strikes, labor disputes and break down of communication system etc.) and which by the exercise of reasonable diligence could not be prevented or provided against and effects of which by could not be overcome by reasonable expenditure.

7-2. The party so affected by an event of force majeure shall as soon as it becomes aware of the occurrence thereof, immediately notify the other party, the party so effected shall do all that is reasonably possible to remove or ameliorate the effect of such an event of force majeure. If all reasonable efforts fail or if the event of force majeure persists beyond a period of thirty (30) days, either party may terminate this Agreement with immediate effect.

8- Governing Law and Jurisdiction

8.1 This agreement shall be governed by and construed in accordance with the laws of the Islamic Republic of Pakistan.

8.2 Disputes arising out of this Agreement are subject to the exclusive jurisdiction of the courts of Islamabad, to which the Parties irrevocably submit.

9- Amendment

This Agreement and schedules thereto shall not be amended except by the mutual consent in writing of both the parties.

10- Assignment

The Contractor shall not assign this Agreement or any of its obligations hereunder, either in whole or any part, to any other person in any form or manner what so ever, without the prior written consent of the Commission.

11- Waiver

The failure of any party to exercise any right or the waiver by any party of any breach, shall not prevent a subsequent exercise of such a right or be deemed a waiver of any subsequent breach of the same or any other provision of this Agreement.

12- Entire Agreement

This Agreement along with the schedules constitutes the entire agreement between the parties in respect of the subject matter hereof and supersedes all prior oral or written arrangements.

13- Severance

If any one or more provisions of this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respects, such provision (s) shall be limited, modified or severed as necessary to eliminate the invalidity, illegality or unenforceability and all other provisions of this Agreement shall remain unaffected.

14- Notice

14-1. Any notice, request or consent made pursuant to this Agreement shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the party to whom the communication is addressed, or when sent by

registered mail, facsimile or electronic mail to such party at the contact details detailed below.

To the Commission:

Securities and Exchange Commission of Pakistan
NIC Building 63, Jinnah Avenue,
Islamabad

Telephone 051-9207092-4 Ext.160
Facsimile: 051-9204915
E-mail:

To the Contractor:
Mr. XYZ
Designation
XYZ (Pvt.) Ltd
Address

Telephone XXX-XXXXXXX
E-mail:

14-2. A party may change its contact details by providing notice thereof to the other party without having to amend this agreement in accordance with this article.

15- Confidentiality

15-1. The Contractor undertakes and shall ensure the complete confidentiality of all and any information in respect of this agreement and the services stated herein, including without limitation the communication to and by the Commission about any of its business information. The Contractor shall not disclose any such information to any person.

15-2. The Contractor shall keep strictly confidential any and all business and technical information that may be disclosed or confided to it by the Commission or which the Contractor or any of its employees / staff may obtain directly or indirectly during the course of performance of this Agreement.

15-3. It shall keep strictly confidential any and all information that may divulge upon it or any of its personnel during the course of performance of this agreement. It shall not disclose any such information to any person or allow utilization of the same in any person. The terms of confidentiality as applicable on the employees of the Commission in terms of SECP Act 1997 shall be applicable on all the staff and personnel of Contractor working in the premises.

15-4. In order to ensure confidentiality, Non-Disclosure Agreement i.e. **Schedule-B,** shall be signed by both the parties.

16- Relationship

The parties hereby agree that no terms of this Agreement shall be construed as to portray and employer-employee relationship between the parties and that both the parties are acting independently and at their entire discretion.

17- Stamp Duty

This Agreement shall be stamped in accordance with Stamp Act, 1899 by the Contractor.

18- Schedules & Annexure

Any and all schedules and annexures to this Agreement shall be deemed to be an integral part of this Agreement and shall be construed accordingly.

In witness hereof the parties hereto have executed this agreement on the date and at the place first above mentioned.

For Securities and Exchange Commission of Pakistan

For XYZ Pvt. Ltd

Name: _____

Title _____

Name: _____

Title: _____

Witness

_____

Witness

_____

SCHEDULE-A of Sample Agreement

Scope of Work entails:

XYZ Pvt. Ltd. is required to conduct vulnerability assessment / penetration testing to determine security weaknesses and vulnerabilities of the Commission's applications and infrastructure. Total number of IPs to be tested will be up to twenty-five (25). The details of IPs will be shared after the award of contract. Four tests are to be conducted by the service provider, with each having an independent report.

Black Box: No prior information will be given to service provider except the target IP addresses.

Grey Box: Limited information of target system e.g. IPs, application URLs and frontend etc. would be provided. Authentication credentials will not be part of provided information.

White Box: Application's authentication credentials will be provided in addition to the information that was provided in the Grey Box testing.

Follow-up: After the submission of above-mentioned testing (Black box, Grey box, and White box) reports, SECP will discuss and implement the security fixes recommended by the vendor in the reports. The service provider will be required to verify these measures by performing associated vulnerabilities testing. SECP will have at least four (04) months to request the follow-up testing.

The penetration testing to be conducted in line with the globally recognized penetration testing standards, such as:

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information System Security Assessment Framework (ISSAF)
- LPT (Licensed Penetration Tester) methodology from EC-Council
- WASC-TC (Web Application Security Consortium Threat Classification)
- PTF (Penetration Testing Framework)
- NIST SP800-115 (Technical Guide to Information Security Testing and Assessment)

The penetration testing approach and risk assessment methodology should be compatible with globally known compliance standards and regulations

The submitted report(s) shall contain:

- Review of the current security state of SECP IT infrastructure/ information assets
- Full methodologies and techniques used during the VAPT project
- A list of deficiencies tied to the system/ process for focused remediation for both internal and external testing
- VAPT report including threats and vulnerabilities to SECP's information assets including probability and impact using/referring industry standards and best practices
- The report should include detailed Description, Evidences, References, CVSS, and Risk Rating Calculation etc.

- Detailed recommended remediation measures for each identified threat, vulnerability and deficiency
- If suggested recommendations for risk mitigation/ removal could not be implemented; alternate solutions to be provided
- An executive report for senior management should also be submitted summarizing the approach, findings, and recommendations
- Explanation how the discovered risks may impact the business and business continuity
- Presentation for the senior management
- A security roadmap for the Commission to ensure compliance and address the security gaps including investments to reinforce IT security
- Final consolidated report after follow up testing of the entire environment

Project Timelines:

- The black box, grey box, and white box testing to be completed within 60 calendar days after the award of contract
- SECP will implement the recommended security fixes within 60 days of receiving the initital report
- Followup testing by the bidder be completed within 30 days of SECP go ahead

Annex – "E"

Sample Non-Disclosure Agreement (NDA)

This agreement is made the on _____ between:

(1) The Information Systems and Technology Department (IS&TD), Securities and Exchange Commission of Pakistan (the "SECP"), NIC Building, Jinnah Avenue, Blue Area, Islamabad

and

(2) Bidder Name, Office Address _____

hereinafter referred to as "Parties" collectively and the party disclosing shall be referred as "Disclosing Party" and the party receiving information shall be referred as "Receiving Party". For the purpose of preventing the unauthorized disclosure of Information as defined below, these parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and information ("Information").

Background:
The Parties wish to discuss investment and collaboration opportunities relating to SECP's Information Systems and Technology Department business models and/or the technical and commercial capabilities of various technologies and projects ("Opportunities and Technologies") developed by one or more of the Parties. The Parties wish to mutually disclose certain Security Classified Information (SCI) to enable each of them to fully assess the Opportunities and Technologies.

It is agreed that:
In consideration for the mutual disclosures, the Parties agree to the terms of this Non-Disclosure Agreement (NDA):

1. "Information" means all information, data, ideas, innovations or material disclosed by any of the Parties relating to the Opportunities and Technologies, whether or not marked or designated as confidential, including, but not limited IS&TD's information to business plans, business proposals, projects, financial information, customer/company lists, prospective customers, technical proposals, product descriptions, hardware specifications, software in both source and object code, computer outputs, computer interfaces, application program interfaces, computer calls, flow charts, data, drawings and know-how.

Each Party's Obligations:

2. Each Party will:
    a. Keep the Information disclosed to it by any disclosing Party confidential and secure, and in addition apply the same degree of care and the same controls which that Party applies to his or its own trade secrets.
    b. Use or make copies of the Information disclosed to it solely to assess the Opportunities and Technologies. Any such copies shall remain the property of the disclosing Party and be distributed or otherwise be made available internally within the receiving Parties on a need to know basis.
    c. Give immediate notice to the disclosing Party if a receiving Party knows of or suspects that there has been any unauthorized use or disclosure of Information arising through a failure by a Party to keep the Information confidential.

Publicity:

3. No receiving Party will without the prior consent in writing of the disclosing Party either release any press statement or issue any other publicity regarding the existence, scope, objective, conduct, performance or results of any proposed or actual contract between any of the Parties.

Exclusions:

4. The provisions of this Agreement shall not apply to Information:
    a. which a receiving Party can prove to the reasonable satisfaction of the disclosing Party was lawfully in his or its possession at the time of disclosure and was not acquired either directly or indirectly from the disclosing Party; or
    b. which is lawfully generally known (other than due to the negligent act or omission of Parties or his breach of this Agreement); or
    c. which the receiving Party obtains from a third party which was entitled to disclose that Information to the receiving Party without any restriction.

Various Obligations:

5. Each receiving Party agree that he or it shall not acquire any right in or title to or license in respect of the Information disclosed to it or any intellectual property rights embodied in the Information. The rights provided to the Parties under this Agreement are personal to the Parties and shall not be assigned or transferred to any other party whatsoever.
6. The obligations under this Agreement shall continue as regards any item of Information until it is lawfully generally known or is otherwise not subject to the provisions of this Agreement. Since the information available with SECP is highly confidential, the receiving party shall never be allowed to disclose such information so the receiving party shall not be allowed to disclose the information even after the expiry of the agreement.
7. On the written request of a disclosing Party at any time, each receiving Party agrees to:
    a. promptly return or procure the return of or destroy (at the disclosing Party's option) all or some (as the disclosing Party may direct) of the originals and copies of the Information under his or its care or control and
    b. confirm in writing that this has been done and that no Information or copies exist under the receiving Party's care or control and
    c. Not use the Information for any other purpose whatsoever.
8. Nothing in this Agreement prevents disclosure of the Information to any persons or bodies having a legal right or duty to have access to or knowledge of the Information.
9. This Agreement constitutes the entire agreement and understanding between the parties with respect to its subject matter and replaces all previous NDA agreements between, or undertakings by the parties with regard to such subject matter. This Agreement cannot be changed except by written agreement between the parties.
10. (i) All disputes arising out of all disputes arising out of or in connection with the present agreement shall be settled through Arbitration. Each Party shall appoint an arbitrator and the appointed arbitrators shall commence the proceedings. In case of difference of opinion between an even number of appointed arbitrators, the matter shall be referred to an umpire mutually appointed by the arbitrators. The umpire shall then make an award which shall be final and binding. Prior to initiation of arbitration proceedings, the aggrieved Party shall give the other Party written notice describing the claim and amount as to which it intends to initiate action.

    (ii) The place of arbitration shall be Islamabad, the arbitration shall be governed by the Arbitration Act, 1940 and the language of the arbitration shall be English.

Signed for and on behalf of
Information Systems and Technology Department, Securities and Exchange Commission of Pakistan

Name:
Designation:

_____

Signed for and on behalf of

Bidders

Name:
Designation:

_____

Witness No. 1:
Name:
Address:
NIC:

_____

Witness No. 2:
Name:
Address:
NIC:

_____