*Government of Pakistan*
PAKISTAN TELECOMMUNICATION AUTHORITY
HEADQUARTERS SECTOR F-5/1, ISLAMABAD.
https://www.pta.gov.pk

Date: February 6, 2026

# EXPRESSION OF INTEREST (EOI)

## HIRING OF SERVICES FOR CYBER SECURITY AUDIT AND VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

### 1. EXECUTIVE SUMMARY

Pakistan Telecommunication Authority (PTA), in carrying out its regulatory and operational mandate, maintains various critical networked systems, databases, infrastructure and digital communication services. These require strict cybersecurity integrity to ensure uninterrupted secure operations.

Through this EOI, PTA intends to engage a qualified and accredited cybersecurity firm that possesses required specialization, knowledge and technical capability to conduct an in-depth Cyber Security Audit and VAPT of PTA's IT and communication ecosystem. intended engagement aims to proactively identify potential vulnerabilities, highlight threat vectors, assess exploitable weaknesses, and provide high-quality recommendations for remediation. end objective is to reinforce PTA's cyber resilience, thereby ensuring digital confidentiality, operational reliability, and institutional trustworthiness.

### 2. DEFINITIONS

i. **"PTA"** refers to Pakistan Telecommunication Authority, procuring entity.
ii. **"Firm"** refers to bidding cybersecurity company submitting an EOI in response to this invitation.
iii. **"Vulnerability Assessment"** refers to process of systematically scanning, detecting and documenting potential security weaknesses.
iv. **"Penetration Testing"** refers to controlled ethical hacking and exploit-based testing aimed at demonstrating real-world attack feasibility.
v. **"Cybersecurity Audit"** refers to detailed examination of existing security controls, policies, monitoring protocols and compliance measures.
vi. **"CTDISR"** refers to Cybersecurity Testing & Data Infrastructure Security Requirements, which may serve as a baseline for this evaluation.
vii. **"OWASP"** refers to Open Web Application Security Project framework widely recognized for application security standards.

ABDUR RUB KHAN
Director (Procurement)
Pakistan Telecommunication Authority
Headquarters, F-5/1, Islamabad

viii. **"Applicant"** refers to an entity participating at EOI stage before final technical and financial bidding.

## 3. BACKGROUND

PTA operates multiple enterprise systems, regulatory platforms, secure communication channels, public service portals, and data repositories, which must remain secure against cyber threats.

Given global trend of increased cyber-attacks, data breaches, malware infections and infiltration attempts, cybersecurity validation has become essential operational hygiene PTA regularly engages independent security experts to evaluate cyber defenses to preserve public trust, institutional credibility, and compliance with legal and regulatory obligations.

## 4. OBJECTIVE OF ASSIGNMENT

i. To detect technical and procedural vulnerabilities in PTA's digital infrastructure.
ii. To determine extent to which vulnerabilities may be exploited by unauthorized entities.
iii. To assess effectiveness of existing technical, administrative and physical security controls.
iv. To conduct both external and internal penetration testing based on globally accepted testing protocols.
v. To recommend both short-term tactical fixes as well as strategic policy-level security improvements.
vi. To conduct follow-up verification of remediation efforts and confirm closure of identified issues to ensure lasting security improvements.

## 5. DETAILED SCOPE OF WORK

### 5.1 IT Infrastructure Security Testing

i. Conduct a complete review of PTA's network segmentation to maintain logical and physical isolation of critical infrastructure.
ii. Examine firewall rulesets, NAT policies, threat-recognition settings and edge device configuration to detect weaknesses.
iii. Review DNS architecture, domain controller security, authentication mechanisms and trust relationships.
iv. Validate correctness and restrictiveness of Access Control Lists (ACLs), ensuring principle of least-privilege.
v. Carry out internal network scanning and enumeration through authenticated and unauthenticated testing.
vi. Detect unauthorized or misconfigured Wi-Fi access points or unauthorized network taps.
vii. Identify protocol-level risks such as outdated cryptographic standards, deprecated protocols, insecure broadcasts etc.

### 5.2 Application-Level Security Testing

a. Perform white-box and black-box testing of PTA web portals and applications.
b. Check for input sanitization weaknesses and vulnerability to injection attacks.
c. Verify credential handling, password policies, brute-force resistance and MFA enforcement.
d. Test for risks associated with session hijacking, token reuse or session fixation.
e. Attempt authentication bypass and privilege escalation to test resilience of access control.
f. Evaluate risks of data leakage during runtime, logging, caching or backup processes.
g. Conduct a complete OWASP Top-10 review including SQL injection, XSS, CSRF, SSRF etc.

### 5.3 Information Storage & Database Security

a. Review user access privileges in live databases to ensure no unnecessary elevated access exists.
b. Simulate SQL injection and related database attack patterns.
c. Evaluate storage of backup archives, verifying encryption and secure retention practices.
d. Assess encryption in-transit and at-rest for sensitive and classified data.
e. Review event logs for anomalies, failed authentication attempts and recording completeness.
f. Verify that storage and classification handling of personal and confidential data meets best-practice standards.

### 5.4 Cloud / Hybrid Infrastructure (if applicable)

a. Conduct container and VM-based infrastructure scanning to detect open ports or insecure configurations.
b. Examine storage of access keys and tokens to ensure protection against credential theft.
c. Validate security of federated trust relationships between services and APIs.
d. Analyze authentication and identity management across multiple service layers.

### 5.5 Policy & Process Audit

a. Review documented cybersecurity Policies and SOPs for completeness and adherence to practice.
b. Assess incident-response maturity concerning detection, tracking and resolution timelines.
c. Evaluate user-privilege assignments, RBAC consistency and dormant accounts handling.
d. Assess employee cybersecurity awareness and associated internal usage protocols.

### 5.6 Final Verification / Retesting

a. Conduct secondary testing after reported vulnerabilities are mitigated.
b. Validate closure of issues and ensure no regression vulnerabilities occur.
c. Provide updated risk indexing and final validated security ratings.

ABDUR RUB KHAN
Director (Procurement)
Pakistan Telecommunication Authority
Headquarters, F-5/1, Islamabad

## 6. COMPLIANCE & AUDIT FRAMEWORKS

i. Cybersecurity audit must align with ISO 27001:2022 standard.
ii. OWASP TOP-10 industry standards for web and API application security must be applied.
iii. ISO-27001 aligned control review methodology is recommended.
iv. Internationally recognized ethical penetration testing practices should be followed to ensure safe execution and trustworthy findings.

## 7. CONFIDENTIALITY OBLIGATIONS

i. firm shall treat all PTA data, system information, architecture documentation, security configurations, internal communications, and discovered vulnerabilities as classified information. No content shall be shared with any external party without explicit written consent of PTA.
ii. All engagement personnel shall adhere to strict confidentiality and non-disclosure protocols, and may be required to sign NDAs if directed by PTA. Security-sensitive information provided to firm must be stored securely, encrypted where required, and must not be retained beyond engagement period.
iii. Any breach of confidentiality obligations by firm or its personnel shall be considered a serious violation of contract terms and may result in legal consequences, contract termination, financial penalties, or blacklisting from future PTA procurements.

## 8. ELIGIBILITY REQUIREMENTS

i. Firm must be legally registered in Pakistan and operating as a recognized technology or cybersecurity service provider. Documentation of registration must be provided with EOI submission.
ii. Firm must be listed on Federal Board of Revenue (FBR) Active Taxpayer List (ATL) and fully compliant with taxation procedures and obligations.
iii. Firm must be recognized as a PTA or National CERT (nCERT) Category-I Cybersecurity Audit entity or possess equivalent cybersecurity accreditation acceptable to PTA.
iv. Firm must have a proven track record of at least Five (5) years in providing cybersecurity services, audits, penetration testing or related security engagements for corporate, financial, governmental or telecom organizations.
v. Firm must demonstrate verifiable history of similar successful engagements, particularly within environments involving sensitive IT systems or regulatory operations. Supporting evidence may include client certificates, completion letters, or testimonials.

ABDUR RUB KHAN
Director (Procurement)
Pakistan Telecommunication Authority
Headquarters, F-5/1, Islamabad

## 9. DOCUMENTS REQUIRED WITH EOI

i. A complete Company Profile describing business history, technical specialization, physical presence, and organizational capability relevant to cybersecurity engagements.
ii. Certified copies of legal registration documents, incorporation certificates, and any relevant regulatory approvals or business certifications.

iii. Tax compliance evidence including ATL status and taxation identification details. CVs of key personnel proposed for engagement, including their professional experience, assigned functional roles, and competency levels. Credentials of lead cybersecurity experts, preferably holding one or more of following: CISSP, CISM, OSCP, CISA, ISO 27001 Lead Auditor certification or equivalent.

iv. Summary of prior engagements of similar scope including project nature, organization type, timeline, and technical achievements.

v. Signed declaration that firm has never been blacklisted by any governmental, military, regulatory or international organization.

## 10. SUBMISSION FORMAT

i. All EOI submissions must be completed in digital format using PPRA/EPADS portal. No physical, couriered or email submissions will be entertained.

ii. File format must be either PDF or DOCX, professionally structured, readable, and clearly organized.

iii. All supporting documentation must be compiled into a single bundled submission or clearly indexed in multiple attachments within EPADS submission interface.

iv. Interested applicants are required to submit their applications via EPADS **by 23rd February, 2026 at 10:30 AM.** The EOI shall be opened on the same day at **11:00 AM.**

## 11. EVALUATION OF EOI

i. PTA will evaluate submitted EOIs through an internal review committee applying objective and transparent evaluation criteria. assessment will focus on institutional financial strength, staffing skillset, technical knowledge, and historical performance.

ii. Relevance and depth of cybersecurity experience, including penetration testing, secure system design, audit reporting proficiency and incident response track record, shall be a central evaluation factor.

iii. Quality and expertise of proposed personnel, including recognized professional certifications, applied cybersecurity competencies and documented experience in similar engagements, shall be reviewed.

iv. Compliance with minimum eligibility requirements and completeness of documentation will determine whether firm proceeds to shortlisting stage.

## 12. POST-QUALIFICATION

i. Only shortlisted firms meeting PTA's technical and compliance expectations shall proceed to subsequent procurement stage. These firms will be issued a formal Request for Proposal (RFP), outlining final defined scope, deliverables, timelines and contractual framework.

ii. During RFP stage, firms will submit a complete technical proposal and a sealed financial bid under procedures compliant with PPRA Single Stage–Two Envelope methodology.

## 13. SECURITY CLEARANCE

ABDUR RUB KHAN
Director (Procurement)
Pakistan Telecommunication Authority
Headquarters, F-5/1, Islamabad

PTA reserves right to conduct background verification and security clearance of key cybersecurity personnel assigned to engagement. This may include identity verification, employment history, prior affiliation review, and professional reputation screening.

PTA may require that some or all engagement personnel be cleared for access to restricted systems or data. In cases of clearance denial, firm must assign alternate eligible personnel approved by PTA.

## 14. OWNERSHIP OF RESULTS

i. All data, logs, test results, audit reports, vulnerability findings, risk assessments, remediation guidance and final technical deliverables shall be exclusive intellectual property of PTA. firm shall not retain backup copies or use project output for internal or commercial purposes.

ii. Any attempt to replicate or share discovered vulnerabilities, system maps or configuration details outside PTA or with third parties will be treated as a confidentiality breach.

iii. PTA reserves right to integrate or archive all findings for future security planning, defense architecture enhancement and compliance documentation.

## 15. GENERAL TERMS

i. PTA retains absolute discretion to accept or reject any EOI without obligation to justify its decision and without incurring liability to any applicant.

ii. Being shortlisted or participating in EOI does not constitute any contractual binding or guarantee of downstream assignment or service award.

iii. No financial quotations, cost projection or invoicing estimates shall be submitted at EOI stage. These will only be considered during RFP evaluation.

iv. PTA will not bear any cost incurred by firms in preparation or submission of EOI documentation. All submission costs remain responsibility of applying firm.

## 16. CONTACT

Any administrative queries regarding EOI submission may be directed to office of:

Director (Procurement)
Pakistan Telecommunication Authority, Headquarters
F-5/1 Islamabad
Tel: 051-2878157

ABDUR RUB KHAN
Director (Procurement)
Pakistan Telecommunication Authority
Headquarters, F-5/1, Islamabad