



**National Telecommunication and Information Technology
Security Board (NTISB)**

Request for Proposal

**For Hiring a Third-Party Evaluation/Validation Firm for Conducting TPV/E
of PSDP Project "Cyber Security for Digital Pakistan (Phase-I) / NCERT"**

GOVERNMENT OF PAKISTAN
National Telecommunication and Information Technology Security Board
(NTISB)

INVITATION TO BIDS

1. Cyber Security for Digital Pakistan /nCERT invites bids for **Hiring a Third-Party Evaluation/Validation Firm for Conducting TPV/E of PSDP Project "Cyber Security for Digital Pakistan (Phase-I) / NCERT"** for which electronic bids are invited under Single Stage-Single Envelope bidding procedure through **e-PADS Version 2.0** from the firms/companies registered with Income Tax, Sales Tax Departments, which are on FBR's Active Taxpayer's List (ATL) and pre-qualified by MoIT&T/MoPD&SI.
2. The prospective service providers are required to submit their electronic bids including technical and financial proposals along with the Bid Security instrument amounting to Rupees 0.5 million/- (Rupees Five Hundred Thousand Only) submitted in favor of Project Director, CSDP/NCERT (FTN/NTN: 9012000-7) through PPRA e-PADS Version 2.0.
3. **E-Bidding documents**, containing detailed terms & conditions, specifications and requirements etc. are available on e-Pak Acquisition and Disposal System (EPADS) at <https://vendors.epads.gov.pk/>.
4. Bidder(s) are required to get themselves registered on **EPADS v2.0** on or before **March 31, 2026 11:00 AM**. E-bids will be opened using **EPADS v2.0** on the same day at **March 31, 2026 11:30 AM**. Manual submission of Bids shall not be entertained. Those vendors who have not yet registered on the new version of **EPADS v2.0**, may register themselves on <https://vendors.epads.gov.pk/>. A tutorial to explain the registration process is available at <https://www.youtube.com/watch?v=MNW6T38v7tc>
5. Original Bid security instrument **MUST** be submitted to the undersigned before closing hours of the bid submission time otherwise respective bid will not be opened.
6. Bidding documents can be accessed from the website of National Cyber Emergency Response Team (<https://pkcert.gov.pk/>) as well as on PPRA website.
7. Bids will be opened on the same day i.e., **31st March, 2026 at 1130 hours** in the presence of representatives of the bidders.
8. As per PPRA Rules 33(1), 2004, National Cyber Emergency Response Team (NCERT) has the right to reject any or all bids/ proposals at any time prior to the acceptance of a bid/proposal.

Deputy Secretary
National Telecommunication and Information Technology Security Board (NTISB)
Cabinet Division, Islamabad
Ph No. 051-9208854
Email: dsntisb@cabinet.gov.pk
Website: (<https://Cabinet.gov.pk/>)

1. Background

1. The Government of Pakistan, recognizing the critical importance of a secure digital ecosystem, has approved and funded the PSDP project **Cyber Security for Digital Pakistan (Phase-I) / NCERT (National Cyber Emergency Response Team)**. This project is a cornerstone of the national cybersecurity strategy, aiming to establish a robust framework to protect the country's digital infrastructure, data, and citizens from escalating cyber threats.
2. The primary objective of the project is to establish a state-of-the-art National Cyber Emergency Response Team (NCERT) with the capability to proactively monitor, detect, prevent, respond to, and recover from cyber threats and incidents. The project's scope is comprehensive, covering key objectives as outlined in its approved PC-1 summary enclosed at **Annex-A**. These include the establishment of the NCERT itself, the development of national cybersecurity frameworks, the setup of Security Operations Centers (SOC), the establishment of screening, forensic labs, capacity building initiatives, and the fostering of international cooperation.
3. Given the strategic importance, technical complexity, and significant public investment in this PSDP project, the National Telecommunication and Information Technology Security Board (NTISB) is committed to ensuring transparency, accountability, and the achievement of its intended outcomes. To this end, NTISB seeks to engage a qualified and independent Third-Party Evaluation/Validation (TPV/E) firm.
4. As per the guidelines of the Planning Commission of Pakistan for development projects, and to ensure an unbiased assessment, NTISB intends to hire a TPV/E firm from the panel of firms pre-qualified by the Ministry of IT and Telecom (MoIT&T)/MoPD&SI. This independent evaluation will provide a critical and objective review of the project's progress, quality, financial management, and, most importantly, its performance against the specific objectives detailed in the PC-1 enclosed at **Annex-A**.
5. This Request for Proposals (RFP) is issued to firms pre-qualified by the MoIT&T/MoPD&SI for providing TPV/E services. The firm selected through this competitive process will conduct a comprehensive and independent evaluation of the "Cyber Security for Digital Pakistan (Phase-I) / NCERT" PSDP project.

2. Objectives of the Assignment

The overall objective of this assignment is to conduct an independent Third-Party Evaluation/Validation (TPV/E) of the PSDP project "Cyber Security for Digital Pakistan (Phase-I) / NCERT" against its approved PC-1.

The specific objectives are to:

- a. Assess the project's progress against its **approved PC-1 objectives** enclosed at **Annex-A**, including physical and financial targets, and identify any deviations or delays.
- b. Evaluate the efficiency and effectiveness of project management, implementation arrangements, and financial controls in achieving these objectives.
- c. Review the technical quality and appropriateness of the goods, services, and works procured and delivered under the project in relation to its stated goals.
- d. Assess the project's governance structure, risk management practices, and compliance with relevant rules, regulations, and approved plans.
- e. Identify implementation challenges, bottlenecks, and capacity constraints that hinder the achievement of the PC-1 objectives.
- f. Provide evidence-based, actionable recommendations for corrective measures, course correction, and improved project management to ensure the successful and timely completion of all project components and the long-term sustainability of its outcomes.

3. Scope of Work / TORs

The TPV/E firm shall be responsible for a comprehensive evaluation covering, but not limited to, the following areas. The evaluation must be structured around the objectives defined in the project's PC-1.

a. Review of Project Design and Framework:

- i. Assess the relevance, clarity, and logical framework of the project objectives/deliverables and their associated outputs/targets as outlined in the PC-1.
- ii. Evaluate the coherence of the project's design, activities, and implementation strategy for achieving these objectives.
- iii. Review the adequacy of the results framework and monitoring indicators linked to each objective.

b. Assessment of Implementation Progress and Performance Against PC-1 Objectives:

The core of this assignment is to validate the status of each of the PC-1 objectives. The firm will:

- i. Conduct a thorough review of physical progress against the specific requirements/targets listed for each objective. This includes, but is not limited to, an assessment of:
 1. **Establishment of National CERT:** Status of HR hiring, renovation of the office building, and to identify risks on a national level, assess them, conduct mitigation activities, and monitor ongoing threats to Pakistan's Digital Landscape through establishment of National CERT.
 2. **Cyber Emergency Response Team:** Progress on the establishment of the National Cybersecurity Operations Center, Cybersecurity Incident Monitoring, Incident Response and Management, National Cyber Incident Coordination Center, and SIEM/SOAR Implementation, etc.
 3. **Governance, Risk, and Compliance:** Evaluation of the development of policies, regulations, and standards, risk assessment & risk management, Critical Infrastructure Defense, Audit & Compliance, and implementation of the National Cyber Security Strategy, Facilitation and consultancy in cyber security controls implementation to Government organizations.
 4. **Capacity Building and Awareness:** Evaluation of the National Cyber Capacity Building Training/Awareness Programs and initiatives, including the ABC Program, Roadshows, Internship Programs, Webinars, and training sessions delivered, and Public-Private Partnerships (Academia and Research Institutions Partnerships, Intra Agency Partnerships, Businesses, Industry, and Government), International Partnerships/Memberships of international CERTs/forums (APCERT, FIRST, etc.)
 5. **Technology Development Centre:** Assessment of development, monitoring, and operations of Vulnerability Disclosure Platform (VDP), Vulnerability Management, Triage Route, and Track Vulnerability Reports, CDO/COO toolkits, and development of a Virtual Training Environment (VTE).
 6. **LABS:** Progress on the establishment of Forensics and Software/Hardware screening labs.
- ii. Evaluate financial management, including expenditure against the budget allocated for each major objective, adherence to financial rules, and the efficiency of fund utilization.

c. Evaluation of Technical Quality and Appropriateness:

- i. Assess whether the technology, systems, and infrastructure being procured and developed (e.g., for the SOC, Screening, & Forensics Labs) are in line with the project's objectives, industry best practices, and national needs.
- ii. Review the technical specifications, procurement processes, and quality assurance mechanisms for all major procurements.

d. Institutional Arrangements and Governance:

- i. Assess the effectiveness of the project's governance structure in overseeing the progress of the objectives.
- ii. Review the coordination mechanisms among NTISB, MoIT&T, NCERT, and other stakeholders (e.g., sectoral regulators, NITB, PTA, etc.)

e. Identification of Challenges and Recommendations:

- i. Identify critical challenges, bottlenecks, and gaps impeding the achievement of specific PC-1 objectives.
- ii. Provide concrete, actionable, and prioritized recommendations for addressing these issues, including suggestions for course correction, to ensure the project meets its intended goals.
- iii. Assess the potential for sustainability of the project's outcomes (e.g., the NCERT's operations) after project completion and provide recommendations for its long-term operationalization and success.

4. Deliverables

The consultant shall submit the following reports in both draft and final versions (hard and soft copies) to the Ministry.

Sr. No.	Deliverables	Purpose/Description	Timeline
1.	Inception Report	Detailed work plan, refined evaluation methodology (including a matrix mapping evaluation questions to the PC-1 objectives), and data collection tools.	2 weeks from date of signing of contract (Payment 20 % of total contract price upon submission of Inception Report)
2.	Interim Progress Report	Preliminary findings based on initial document review and stakeholder consultations, providing an early overview of progress against key objectives.	4 weeks from date of signing of contract (Payment 20 % of total contract price upon submission of Interim Progress Report)

Sr. No.	Deliverables	Purpose/Description	Timeline
3.	Draft TPV/E Report	Comprehensive report covering all aspects of the Scope of Work. This report must include a detailed section-by-section analysis of the status of all PC-1 objectives , complete with findings, analysis, conclusions, and preliminary recommendations.	8 weeks from date of signing of contract (Payment 30 % of total contract price upon submission of Draft TPV/E Report)
4.	Final TPV/E Report	Finalized report incorporating feedback from NTISB and MoITT on the draft, with clear, actionable recommendations for project improvement, course correction, and long-term sustainability. An executive summary must highlight the overall achievement level of the PC-1 objectives.	12 weeks from date of signing of contract (or 2 weeks after receipt of feedback on draft) (Payment 30 % of total contract price upon submission and acceptance of Final TPV/E Report from NTISB)

5. Proposal Submission Requirements

Interested firms, pre-qualified by the MoIT&T/MoPD&SI for TPV/E services, are invited to submit their proposals. Technical and Financial proposals must be via the government's e-procurement portal PPRA E-PADS 2.0 as specified.

Technical Proposal must include:

- i. **Understanding of the Assignment and TORs:** Demonstrated comprehension of the NCERT project and its PC-1 objectives.
- ii. **Detailed Methodology and Work Plan:** A clear approach for evaluating the complex, multi-faceted objectives of the project.
- iii. **Team Composition, with CVs of key experts:** (Team Leader, Cyber Security Specialist, Procurement/Financial Management Specialist, M&E Specialist).
- iv. **Relevant Past Experience:** Particularly in evaluating large-scale IT/Telecom or public sector infrastructure projects with clearly defined, multiple objectives. Provide references.

- v. **Quality Assurance and Data Validation Procedures.**
- vi. **Proof of being pre-qualified by the MoIT&T/MoPD&SI for TPV/E services.** (Mandatory)

Financial Proposal must include:

- i. Detailed cost breakdown (professional fees, travel/accommodation, data collection, workshops, report printing, taxes, etc.).
- ii. Total bid amount in Pakistani Rupees (PKR).
- iii. Required Bid validity period is 120 days.

6. Evaluation and Scoring Criteria

Proposals will be evaluated using a Quality and Cost-Based Selection (QCBS) method, with a weight of 70% for the Technical Proposal and 30% for the Financial Proposal.

Only firms that are **pre-qualified by MoIT&T/MoPD&SI** and obtain at least **70% marks (Minimum 49 marks out of 70)** in the technical evaluation will qualify to have their financial proposals opened and considered.

6.1. Technical Evaluation (Total 70 Points)

Detailed Marking Methodology for Technical Evaluation is enclosed at **Annexure-B**.

6.2. Financial Evaluation (30% Weightage)

The financial proposals will be opened only for firms that score ≥ 70 points in the technical evaluation.

The lowest-priced financial proposal (**Ls**) will receive the maximum financial score of **100 points**. Scores for other proposals will be calculated as:

$$\text{Financial Score (Sf)} = 100 \times (\text{Ls} / \text{L})$$

Where:

- **Ls** = Lowest evaluated price
- **L** = Price of the proposal being evaluated

6.3. Combined Final Score

The final score will be computed as:

$$\text{Final Score} = (\text{St} \times 0.70) + (\text{Sf} \times 0.30)$$

Where:

- **St** = Technical Score
- **Sf** = Financial Score

The firm achieving the highest combined final score will be recommended for the award of the contract, subject to successful contract negotiations.

7. Confidentiality and Ownership

All data, reports, information, and documents collected, generated, or provided during the assignment shall remain the sole property of the Government of Pakistan and MoITT. The selected firm shall maintain strict confidentiality and shall not disclose any information related to the assignment to any third party without prior written consent from MoITT.

8. Conflict of Interest

The selected firm must operate with complete independence and impartiality. Any firm with a potential conflict of interest (e.g., having provided consultancy services for the design or implementation of the same project, or having a commercial relationship with any of the project's vendors/contractors) must fully disclose this in their proposal. NTISB reserves the right to assess any disclosed conflict and determine the firm's eligibility for the assignment. Non-disclosure of a potential conflict of interest may lead to immediate disqualification.

9. Right to Reject

The National Telecommunication and Information Technology Security Board, Government of Pakistan reserves the right to reject any or all proposals at any stage of the procurement process without assigning any reason.

9. Award of Contract:

Bidder having scored highest marks in Final evaluation as per para-6.3, will be awarded the contract. After acceptance of Technical and Financial bid, an Award Letter shall be issued, in duplicate, to the successful bidder, and the selected Firm, within 15 days of receipt of Award Letter, sign and return the duplicate copy of the Award Letter in acknowledgement thereof. In the event the duplicate copy of the Award Letter duly signed by the Firm is not received by the stipulated date, the Authority may, unless it consents to extension of time for submission thereof, cancel the Award Letter issued to it.

- a. A Performance Bank Guarantee (PBG) from a bank for an amount equal to 10% (10 PERCENT) of the bid/contract price in PAK RUPEE, shall be submitted before signing the contract for carrying out the assignment. For the purpose of Bank Guarantee, the bid/contract price will mean the total bid amount as provided in Financial Proposal.
- b. PBG shall be released subject to final submission and acceptance of **Final TPV/E Report** by NTISB within 12 weeks from signing of contract.

10. Mailing Address/ Contact Information:

The following address details can be used for any correspondence, queries, clarification,

and communication purposes via email and/or telephone calls:

Address	National Cyber Emergency Response Team (nCERT) HQ's, L- Block, Pakistan Secretariat, Islamabad
Telephone	051-9203421-22
Email	bid@pkcert.gov.pk
Website	www.pkcert.gov.pk

Project Brief Objectives/Scope:

Establishment of a National CERT (NCERT) to safeguard Pakistan's digital landscape against cyber threats and to enhance cyber defense, strengthen governance, secure internet services, protect critical infrastructure, develop assurance frameworks, foster public-private partnerships, advance R&D, build national capacity, raise cybersecurity awareness, promote global cooperation, and establish cybercrime response and regulation.

Project Objectives:

1. Identify risks on a national level, assess them, conduct mitigation activities, and monitor ongoing threats to Pakistan's Digital Landscape through the establishment of the National CERT.
2. Creating National standards and a framework, focused on adopting best practices to harden and protect the core infrastructure in telecommunications and internet systems, financial systems, transportation systems, and other critical infrastructures and high-value assets.
3. Create an auditing and licensing mechanism with NTISB that ensures compliance with National standards and cyber policies through risk assessment of digital assets.
4. Stability of National authorities and the ability to ensure they have the necessary human capital base in the form of cyber security engineers, professionals, and technicians, the right investment in Research and Development (R&D) for next-generation cyber security technologies, and for developing indigenous cyber solutions with an overall goal of making Pakistan self-reliant in cyber technologies.
5. Help develop a resilient National Cyber posture.
6. Development of a national-level Cyber Incident Response strategy.
7. Initiate the process of National Cyber Capacity Building.
8. Cyber security operations at the National level to link information sharing and analysis centers across diverse sectors such as financial services, banking, retail, etc. (Public-Private Partnerships). This will facilitate working-level day-to-day coordination against current threats and coordinate incident response activities at the national level.
9. Develop a culture of Cyber Security in Pakistan and increase awareness in the public and private sectors.
10. Leverage and contribute to existing knowledge and best practices developed by International Organizations by joining the International Cyber Security community, and by forming partnerships with local academia and industry.
11. To enhance KPIs such as training 5,000+ individuals via a Learning Management System, reducing misinformation by 30% through new media initiatives, and reducing Mean Time to Respond (MTTR) for cyber incidents with shift-based monitoring.
12. To ensure integrity of ICT products, systems, and services by establishing a mechanism of testing, screening, forensics, and accreditation.

Detailed Marking Methodology for Technical Evaluation

For each sub-criterion, marks shall be awarded based on the qualitative assessment described below. The Evaluation Committee shall assign marks within the prescribed range according to the strength of the proposal.

Sr. No. 1.1 – Understanding of Project Context, NCERT Role & PC-1 Objectives (06 Marks)

Description	Marks Range
Comprehensive understanding of project context, strategic importance of NCERT, and clear articulation of all PC-1 objectives with interlinkages	4–6
Adequate understanding with minor gaps in linking objectives to evaluation requirements	2–4
Basic understanding; lacks depth or clarity on certain objectives	0–2

Sr. No. 1.2 – Methodology (Clarity, Feasibility & Comprehensiveness) (10 Marks)

Description	Marks Range
Clear, structured, feasible, and comprehensive methodology with a detailed evaluation framework	8–10
Well-defined methodology with minor gaps in tools, sequencing, or objective coverage	5–7
General methodology provided; lacks detail in implementation or objective mapping	3–4
Vague, impractical or incomplete methodology	0–2

Sr. No. 1.3 – Innovation & Analytical Rigor (5 Marks)

Description	Marks Range
Strong analytical framework; effective use of mixed methods, benchmarking, or innovative tools	4–5
Some analytical depth; limited innovation	3
Minimal innovation; conventional approach only	1–2
No analytical rigor demonstrated	0

Sr. No. 2.1 – TPV/E or Similar Experience (10 Marks)

Description	Marks Range
Extensive experience (5+ similar large-scale technology projects), including national-level assignments	8–10
Relevant experience in 3–4 comparable assignments	5–7
Limited experience (1–2 relevant assignments)	1–4
No relevant or comparable experience	0

Sr. No. 2.2 – Experience with Government / PSDP / Donor Projects (07 Marks)

Description	Marks Range
Significant experience with Ministries, PSDP projects or multilateral organizations	5–07
Moderate experience with public sector or donor-funded projects	3–5
Limited exposure to government or donor assignments	0–3

Sr. No. 3.1 – Team Leader / Evaluation Expert (8 Marks)

Description	Marks Range
Advanced degree; 12+ years relevant experience; led multiple similar evaluations	6–8
Meets minimum qualification with 10+ years relevant experience	4–6
Below ideal experience or limited similar assignments	1-4
Does not meet minimum criteria	0

Sr. No. 3.2 – Cyber Security Specialist (5 Marks)

Description	Marks Range
Recognized certifications (CISSP/CISM or equivalent) with extensive experience	4–5
Relevant certifications with moderate experience	2–3
Basic certifications or limited exposure	0-1
Lacks required certification or relevant experience	0

Sr. No. 3.3 – Procurement / Financial Management Specialist (5 Marks)

Description	Marks Range
Strong audit/evaluation experience; thorough knowledge of public procurement systems	4–5
Relevant audit/financial evaluation experience	2–3
Limited exposure to procurement or financial systems	0-1
No relevant experience	0

Sr. No. 3.4 – Monitoring & Evaluation (M&E) Specialist (5 Marks)

Description	Marks Range
Extensive experience designing results frameworks and monitoring systems	4–5
Relevant M&E experience in development projects	2–3
Basic exposure to M&E functions	0-1
No relevant experience	0

Sr. No. 4.1 – Work Plan & Timelines (5 Marks)

Description	Marks Range
Detailed and realistic schedule aligned with evaluation objectives	4–5
Clear timeline with minor sequencing gaps	2–3
Basic work plan; lacks milestone clarity	0-1
Unrealistic or incomplete work plan	0

Sr. No. 4.2 – Quality Assurance & Coordination Mechanism (4 Marks)

Description	Marks Range
Strong QA framework, data validation mechanisms and coordination strategy	3-4
Adequate QA and coordination mechanisms	1-3
Limited QA measures described	0-1