REQUEST FOR EXPRESSION OF INTEREST
[DIGITAL ECONOMY ENHANCEMENT PROJECT (DEEP)]

Credit No: 7514-PK

Assignment Title: Consultancy Services for assessment of the Pakistan's cybersecurity infrastructure, sectoral readiness, and recommendations for improvement**.**

Reference No.: PK-MOITT-519715-CS-QCBS

The Ministry of Information Technology and Telecommunication in collaboration with the World Bank is implementing Digital Economy Enhancement Project (DEEP) worth USD $77.73 Million. The main objective of the Program is "to enhance the Government's capacity for digitally enabled public services delivery for citizens and businesses".

In this connection, DEEP intends to hire the consultancy services ("Services") for assessment of the Pakistan's cybersecurity infrastructure, sectoral readiness, and recommendations for improvement**.**

The detailed Terms of Reference (TOR) are attached to this Request for Expression of Interest OR can be found at the following website: (www. moitt.gov.pk) OR can be obtained at the address given below.

The attention of interested consulting firms is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" September 2023 revised February 2025, setting forth theWorld Bank's policy on conflict of interest.

Consultants may associate with other firms to enhance their qualifications but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

A Consulting firm will be selected in accordance with the **Quality Cost Based Selection (QCBS)** method set out in the Procurement Regulations of the World Bank for IPF Borrower September 2023 revised February 2025.

Further information can be obtained at the address below during office hours i.e. 08:30 to 16:30 hours.

Expressions of interest must be delivered (in person, or by mail, or by e-mail) not later than **1400 Hours on December 15, 2025.**

Program Office DEEP
7th Floor Kohsar Block, Pak Secretariat, Islamabad
Deep.consultant@moitt.gov.pk
051-9215347

Terms of Reference (ToRs) for assessment of the Pakistan’s cybersecurity infrastructure, sectoral readiness, and recommendations for improvement.

1. Background

The Ministry of Information Technology and Telecommunication (MoITT) is the national focal Ministry and enabling arm of the Government of Pakistan for planning, coordinating, and directing efforts to initiate and launch IT & Telecom programs and projects aimed at the economic development of the country. MoITT plays a critical role in the development and growth of the country's IT and Telecom sectors. MoITT intends to restructure its organization to cope with global challenges to enhance efficiency, foster innovation, and achieve greater prosperity amidst a competitive globe with vibrant and emerging technological trends.

Digital Economy Enhancement Project (DEEP) is a World Bank-assisted project to enhance the Government’s capacity for digitally enabled public service delivery for citizens and businesses. MoITT is the sponsoring agency of the project with execution support of (i) the Board of Investment (BoI), (ii) the National Database and Registration Authority (NADRA), (iii) the National IT Board (NITB), and (iv) Ignite – National Technology Fund.

DEEP primarily aims to develop key Digital Public Infrastructure (DPI) services supporting the country’s digital economy and society in line with the Digital Pakistan Policy (2018), which calls for the establishment of a holistic, government-wide enterprise architecture and the integration of government services and systems. Development of DPI will support the responsible data exchange, digital authentication, and verifiable credentials—and digitalization of public services (including making them available through a new national portal), which will improve the accessibility and delivery of services, economic opportunities, and social protection. It will also bolster the country’s resilience and adaptability in the face of potential shocks, such as pandemics and recurring climate-induced disasters, to enable the government to deliver cash and other emergency assistance more rapidly and efficiently.

In addition to the citizen's services, DEEP will support: (1) Establishing a catalog of all federal and provincial business RLCOs along with recommendations for simplifying, streamlining, and improving existing regulatory requirements for business investments and operations (2): Designing and developing of the PBP acting as an interface to host all digitalized and available RLCOs; (3): Supporting federal, provincial, and sub-level public sector entities in digitalizing regulatory approvals; (4): Institutionalizing the reform process, exploring financial and institutional sustainability, and management and upgrading of PBP; and (5): Organizing communication and change management activities for transition to the PBP and dissemination of information about the availability of online approvals of RLCOs.

2. Objective

This consultancy aims to engage a highly qualified consulting firm to conduct a comprehensive assessment (gap analysis) of Pakistan's cybersecurity infrastructure, and sectoral readiness/existing posture, and provide actionable recommendations in line with national policies, regulations and international best practices. The consultancy will also develop legal frameworks including but not limited to revising the National Cyber Security Policy (2021)/Strategy, Draft for Cybersecurity Act, and a Regulatory Framework for Critical Information Infrastructures (CIIs).

3. Scope of Work

The consultant's expertise is needed for the following:

A. Assessment:

i. **Cybersecurity Infrastructure:**

- **Review Existing Infrastructure:** Review the current state of cybersecurity infrastructure across government agencies, CIIs, and the private sector.
- **Gap Analysis:** Identify gaps in legal frameworks, institutions, technology, human resources, processes, and policies while comparing them with international best practices
- **Risk Assessment:** Evaluate and prioritize potential cybersecurity threats and vulnerabilities to CIIs and screening of Equipment (Electronic/ IT) and other infrastructure be conducted through CCPL.
- **Risk Management:** Assist/guide Government agencies/CIIs in their Risk Management efforts.

ii. **Sectoral Readiness:**

- **Sector Identification:** Identify Critical Infrastructures (CIs) w.r.t national security and socio-economic stability (e.g., finance, energy, healthcare, IT and Telecommunications etc.).
- **Readiness Evaluation:** Assess the information, and IT/OT and IoT security readiness of each CI, focusing on regulatory/policy frameworks, technical capabilities, incident prevention, detection, and response mechanisms.
- **Stakeholder Consultation:** Engage with stakeholders to gather insights on existing challenges and capabilities.

iii. **Global Cybersecurity Index (GCI) (and other international Indexes on cyber security) Improvement:**

- **Benchmarking:** Compare Pakistan's current GCI ranking with global and regional peers to identify areas of improvement.
- **Strategic Recommendations:** Provide recommendations for improving Pakistan's GCI score, focusing on synergizing efforts/ initiatives in line with ITU's GCI Assessment Criteria.

- **Action Plan Development:** Develop an action plan for further enhancing Pakistan's GCI ranking with a focus on stakeholder multi-stakeholder approach

B. **Revision of National Cyber Security Policy/Strategy:**

- **Vision and Objectives:** Review/redefine the vision and objectives for Pakistan's national cyber security strategy considering zero trust architecture in light of the National Cyber Security Policy 2021.
- **Strategic Priorities:** Identify key priorities such as capacity building, public-private partnerships, incident response, and international cooperation and cyber security in the post-generative AI era.
- **Implementation Framework:** Develop an implementation framework with timelines, responsible entities, and Key Performance Indicators (KPIs).

C. CIIs Identification & Grading Criteria:

In line with PECA-2016 & CERT Rules-2023, as well as sectoral regulations (e.g. PTA Critical Telecom, Data and Information Security Regulations – CTDISR) provide standards for identifying and documenting the Critical Cyber Assets associated with the Critical Assets that support reliable operation of the Critical Infrastructures that require regulatory oversight.

D. International Cooperation/Cyber Diplomacy

Considering 'UN-Norms, Confidence Building Measures', NIST standards and national legislations (PECA-2016, CERT Rules-2023 etc), the development of the following:

- **Agreements/MoUs**
  Draft templates/specified domains that refer to any officially recognized national or sector-specific partnerships i.e., the cooperation or exchange of information, expertise, technology, and other resources across borders with, or regional entity i.e i) **Bilateral (**other foreign government/entity/agency**), ii) Regional entity, iii) M**ultilateral foreign governments or international organizations, iv) Mutual Legal Assistance Treaty (MLAT) / Conventions
- **Domestic Inter-Agency Consultation Framework**: While reviewing the existing hierarchy of national stakeholders dealing with cybersecurity propos~~ed~~ a framework of 'Domestic Inter-Agency Consultation' on cyber security cooperation, diplomacy & information/cyber threat intelligence sharing, specially while executing international MoUs/MLAT/Conventions

E. Legal Frameworks Development:

ii. **Cyber Security Act:**

- **Legal Review:** Review existing cybersecurity-related laws including PECA-2016 and regulations in Pakistan.
- **International Best Practices:** Benchmark against international standards in cybersecurity legislation and Gap Analysis.
- **Need Assessment for establishment of** National Cyber Security Authority (Council.
- **Enhancement of cybersecurity ecosystem against the emerging threat landscape including those revolving around AI, blockchain, dark web, cloud, etc. Develop a comprehensive SOAR (security orchestration, automation and response) based solution for enhanced threat intelligence accordingly.**
- **Broad Parameters:** In line with the Gap Analysis, draft Cyber Security Act addressing i) important definitions (terms & terminologies related to cyber/computer/network security), ii) risk assessment/management requirements, iii) CIIs & data protection, iv) breach notification/incident reporting, v) detection, response and recovery requirements, vi) cybersecurity certification/standardization (national, international and industry) requirements, vii) implementation of cybersecurity measures/regularity compliance, viii) cybersecurity audit requirements, ix) privacy protection, x) e-safety & child online protection, xi) digital signatures and e-transactions, xii) cybersecurity metrics/KPIs, xiii) liability of internet & DNS service providers, xiv) disciplinary actions/penalties/punishments against negligence/breaches/non-compliances and xv) international cooperation (adherence to UN Norms/CBMs/Conventions). In addition, the establishment, functions, and powers of a National Cyber Security Entity (Authority/Council).

iii. **Rules/Regulation/Guidelines under the Cyber Security Act:**

- **Rules for National Cyber Security Entity (Authority/Council)**: Board of Governance, organisational structure, roles and responsibilities including Secure Data Exchange Layer, Enterprise architecture framework, underlying organizations and their roles and responsibilities.
- **Information Security Management Systems**: Provide guidelines to enable organizations to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties
- **Principles and Practices for Securing Information Technology Systems**: Baseline that organizations can use to establish and review their IT security programs.
- **Security in the emerging cyber security threat landscape:** Provide guidelines and solutions for securing cyber space in the post generative AI era.
- **Post quantum Cryptography**: Provide a framework for the development of cryptographic solutions that are quantum proof in the post quantum world by following the NIST international standards for the post quantum cryptography.

- **Risk Assessment/ Management Framework**: Provide the standards/specifications of best practices for an Information Security Management System and risk-based approach to corporate information security risk management that addresses people, processes, and technology.
- **Security by Design(SBD)/Privacy Enhanced Techniques(PETs)**: Provide and develop the framework for the security by design and promote the establishment of PETs for the enhanced security and privacy.
- **Data Protection & Privacy Controls to Federal Information Systems**: Catalog and a process for selecting controls to protect an organization's operations, assets, individuals, other organizations, and the Nation from a diverse set of threats including human error, hostile cyber-attacks, natural disasters, structural failures, and data breaches among others.
- **Hardening Implementation Guidelines**: Contain configuration standards /technical guidance to 'lockdown' Federal information & Assurance-enabled devices systems/software that might otherwise be vulnerable Cyber-attack.
- **Digital Identity Guidelines**: These are for implementing digital identity services, including identity proofing, registration, and authentication of users.
- **CIIs Cybersecurity Framework:** Help public/private sector organizations that provide critical infrastructure with guidance on how to protect it and control baselines for ensuring a compliance monitoring process, along with relevant protections for privacy and civil liberties**. (Just like PTA's CTDISR for telecom sector).**
- **Guide to Industrial Control System (ICS) Security**: Describe how to secure multiple types of Industrial Control Systems against cyber-attacks while considering the performance, reliability, and safety requirements specific to ICS.
- **Guidelines on Implementation of PCI DSS**: Implementation of information security standards for organizations that handle branded credit cards from the major payment card schemes.
- **Compliance and Enforcement:** Propose mechanisms for ensuring compliance, including monitoring, audits, and penalties.

iv. **Public Private Partnership (PPP):** Taking into account 'Pakistan Cloud First Policy' a long-term contract/Service Level Agreement (SLA) between a government/ public sector entity and a private party for providing cybersecurity products or services, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance**.**

F. Capacity Development Framework:

- **Need Assessment:** Conduct a comprehensive need assessment exercise with input from all the relevant stakeholders. Accordingly, develop an action plan for capacity building in line with a focus on the following areas:
- **General Awareness Programs:** Supported with Gap Analysis, recommend and design initiatives and awareness sessions of cybersecurity to equip the target audience with understanding the technology, the risk and the socio-economic and political implications; the target audience includes: a) the Public/Private sector in general, b) Population / Citizens in general, c) Micro, Small and Medium businesses (MSMEs), d) Public sector agencies at local, municipal, and national levels, e) Civil society (Non-Governmental/Not-For-Profit

Organisations), f) Older persons (elderly), g) Persons with specific needs including persons with disabilities, h) Parents, educators, and children as part of Child Online Protection (COP) efforts, i) Legal Community

- **Training & Skill Development Programs (Professionals):** Supported with Gap Analysis, recommend a set of internationally recognized certifications inclusive of all domains of cybersecurity, hands-on training/ workshops and Cyber Drills/CTF Competitions (Blue & Red Teaming) to equip CIIs stakeholders, CERTs, Public & Private organizations with skills to deal with cyber security incidents (preventing, detecting, reporting, handling/mitigating and recovering).
- **Educational Programs for Youth:** Supported with Gap Analysis, recommend short diplomas, graduation and post-graduation degree program curriculums in line with the latest trends/emerging technologies and bridge the industry-academia gap/supply chain.
- **Cybersecurity Research and Development (R&D) Programs:** Supported with Gap Analysis, suggest measures for the investment into national cybersecurity research and development programs at institutions that could be private, public, academic, non-governmental, or international.
- **National Cybersecurity Industry Promotion Program**: Supported with Gap Analysis, suggest incentives whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, to drive the growth of cybersecurity-related products & services, startups/enterprises in the private sector.
- **Cybersecurity services/software exports**: Since Pakistan's cybersecurity exosystem is improving considerably, there is a growing demand for software and services in this sector leaving thereby huge potential for exports. Hence, assess and prepare an action plan accordingly.

G. Stakeholder Engagement:

- **Consultation Forums:** Facilitate seminars, and round-table conferences engaging government agencies with industry stakeholders (national/international), think tanks/ Research & Strategic Organizations, and Civil Society for revisions of existing or development of legal/institutional frameworks for new/emerging technologies.
- **Communication Materials:** Develop materials (templates) to inform stakeholders about the assessment process and benefits.

4. Deliverables

The Consultant will deliver the following:

- **Inception Report:** Summarize the initial assessment, including a SWOT analysis, proposed methodology, and detailed work plan.

- **Interim Assessment Report:** Referring to 'Scope A', provide preliminary findings, including data analysis and initial insights into the current state of cybersecurity, gaps, and opportunities.

- **Draft Cybersecurity Strategy:** Referring to 'Scope B' A comprehensive document outlining the national cybersecurity strategy, including vision, objectives, and an implementation framework.

- **Draft CII Identification & Grading Criteria:** Referring to 'Scope C'**.**

- **International Cooperation/Cyber Diplomacy:** Referring to 'Scope D', submit draft templates of MoUs/ MLAAs & a Domestic Inter-Agency Consultation Framework'**:**

- **Drafts for Legal Frameworks:** Referring to 'Scope E'

  - **Draft Cybersecurity Act**.

  - **Draft Rules/Regulations/Guidelines:** In subsequent phases/order of priority as identified in the 'Interim Assessment Report'.

  - **Draft SLA (PPP).**

- **Final Reports:** Incorporate stakeholder feedback and provide finalized documents for the Cybersecurity Strategy, CIIs identification & Grading Criteria, International Cooperation Strategy, Cybersecurity Act, and subsequent Rules/Regulations/Guidelines.

- **Capacity Development Framework:** Referring to '**Scope F**', submit a detailed report and recommendations.

- **Stakeholder Engagement Report:** Referring to '**Scope G**' document outcomes/minutes of consultation sessions and feedback.

5. Consulting Firm Qualifications

- The firm must have personnel with advanced degrees in cybersecurity, law, public administration, or related fields.
- Proven experience in conducting cybersecurity assessments and strategy development.
- In-depth knowledge of the Pakistani cybersecurity landscape, including legal frameworks and sectoral dynamics.
- Demonstrated success in leading similar assignments or projects at the national or international level with three completed national/international cybersecurity strategies/assessments in the past 5 years.
- Experience with international benchmarks (ITU GCI, ISO audits, NIST CSF) and demonstrated capability in emerging domains (AI-driven threats, post-quantum cryptography, cloud/OT security.
- Must have recognized in cybersecurity certifications.
- Strong capabilities in data collection, qualitative and quantitative analysis, and risk assessment.
- Experience in engaging with diverse stakeholders, including government agencies, industry players, and civil society.

- Excellent communication, presentation, and report-writing skills.
- Fluency in English and Urdu is essential for effective communication and report writing.

6. Reporting

The Consulting Firm will report directly to a designated MoITT official and will be expected to attend regular meetings to provide progress updates and address any questions or concerns. Regular progress updates and reporting requirements to ensure transparency and accountability.

7. Duration of the Assignment

The consultancy is expected to be completed within [12] months, with the possibility of extension based on mutual agreement.

8. Key Team Personnel should include but not be limited to

S#	Position / Role	Minimum Qualification	Relevant Experience
1	Project Head/Cybersecurity Lead	Minimum 16 years of education in Cybersecurity / Information Security or relevant field.	10+ years in national-level cybersecurity projects
2	Legal/Policy Expert	LL.B. or Minimum 16 years of education in Law or Public Policy	8+ years in drafting ICT/cybersecurity legislation
3	Technical Expert (Infrastructure & Risk)	Minimum 16 years of education in IT, CS or relevant field.	7+ years in cybersecurity risk assessment
4	Capacity Development / Training Specialist	Minimum 16 years of education in HR / ICT or related field.	5+ years in cybersecurity training program design