DIGITAL ECONOMY ENHANCEMENT PROJECT - DEEP

TERMS OF REFERENCE SECURE SOFTWARE DEVELOPMENT AND APPLICATION SECURITY EXPERT

A. Background

The National Database and Registration Authority (NADRA) in collaboration with The World Bank and MOITT intends to execute the Digital Economy Enhancement Project (DEEP) approved by ECNEC on 6th April,2023 and funded by The World Bank.

The project aims to digitalize key public services and important registries to transition from a siloed approach toward more integrated service delivery. NADRA has been selected to implement key technological components of DEEP Project i.e., Design and Establishment of National Data Exchange Layer (NDEL) and building for Digital authentication and Verifiable credentials (Digital ID /Vaults) and associated ecosystem.

B. Project Description

Digital Economy Enhancement Project (DEEP) aims at building the capacity of the government to develop key digital public infrastructure (DPI) services supporting the country's digital economy and society in line with the 2018 Digital Pakistan Policy, which calls for the establishment of a holistic, government-wide enterprise architecture and the integration of government services and systems. The project will support the development of DPI—including for responsible data exchange, digital authentication, and verifiable credentials—and digitalization of public services (including to make 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 citizens services, DEEP will support: (1) Establishing a catalogue of all federal and provincial business RLCOs and producing recommendations for simplifying, streamlining, and improving existing regulatory requirements for investing and operating business; subcomponent (2): Designing and development of the PBP acting as an interface to host all digitalized and available RLCOs; subcomponent (3): Supporting governmental, provincial, and local entities in digitalizing regulatory approvals; subcomponent (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.

C. Objectives of Consultancy

The Secure Software Development and Application Security Expert will play a major role in implementing the Secure Software Development Lifecycle (SSDLC) for the project. The expert will also implement the security evaluation and testing mechanisms for the developed code, applications and APIs. The expert will provide hands-on implementation, guidance, technical

expertise and practical support towards the development and implementation of SSDLC and application security mechanisms for the project.

D. Responsibilities

The Secure Software Development and Application Security Expert will be responsible for the following tasks:

1. Conduct threat modelling for applications and APIs to analyze potential security risks and preparation of countermeasures.
2. Design, develop, and manage secure CI/CD pipelines and assist in integrating latest security tools in the pipeline.
3. Perform continuous application testing using Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Interactive Application Security Testing (IAST) methods.
4. Perform continuous Software Composition Analysis (SCA).
5. Perform penetration testing tasks using modern techniques and tools for the entire software ecosystem.
6. Establishment of complete vulnerability assessment and patch management lifecycle in the organization.
7. Other associated responsibilities as per the requirement.

E. Deliverables

The expert will be expected to deliver the following:

1. Complete design, implementation, configuration and operations enablement of SSDLC and Application Security processes of the project.
2. Comprehensive documentation pertaining to the design, implementation, configuration and operations of the corresponding SSDLC and Application Security mechanisms.

F. Timeframe and Supervision

The expert will work for over a period of 1 year (extendable as per the requirement of the project) under the supervision of Cybersecurity Operations and Architecture Specialist.

G. Qualifications and Experience

1. Bachelors in Computer Science / Information Security or related field.
2. At least 07 years of post-bachelor's degree experience in Vulnerability Assessment and Penetration Testing, DevSecOps, Secure Software Development Lifecycle, Application/API Security or similar endeavors.
3. Preference will be given to candidates with OSCP or equivalent certifications.
4. Good knowledge of NIST Secure Software Development Framework (SSDF) and Microsoft Security Development Lifecycle (SDL).
5. Good knowledge of OWASP standards, guidelines and best practices.