REPUBLIC OF KENYA

ICT Authority

COUNTRY: KENYA

PROJECT: KENYA DIGITAL ECONOMY ACCELERATION PROJECT (KDEAP)

IMPLEMENTING AGENCY: Information and Communications Technology Authority (ICTA)

PROJECT ID: P170941; Credit Numbers 7289-KE and 7290-KE

TERMS OF REFERENCE FOR:

Request for Expression of Interest

for

Digital Information Security Expert

Contract No: KE-ICTA-392523-CS-INDV

Issue Date: 6th August 2024

Closing Date: 23rd August 2024

Client:
The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke , info@icta.go.ke
Website: www.icta.go.ke

1. Background

The Government of the Republic of Kenya (GoK) has received financing in the amount equivalent to US$390 Million from the World Bank towards the cost of the first phase of the Kenya Digital Economy Acceleration Project[1] and it intends to apply part of the proceeds to payments for goods, works, non-consulting services and consulting services to be procured under this project.

The project will include the following components.

1.1 Component 1: Digital Infrastructure and Services-The aim of this component is to increase access to high-speed internet for individuals, industry, and government—the 'foundation of the foundations' of a digital economy and strengthen Kenya's role as regional digital leader—while leveraging investments from the private sector

1.2 Component 2. Digital Government and Services- This component will invest in the foundational digital services, platforms, architectures, and policies needed to transform the way the Government communicates and conducts its internal operations.

1.3 Component 3. Digital Skills and Markets- This component aims to equip young Kenyans with digital skills and strengthen their abilities to access and compete in domestic and regional markets through supporting skills development, to study mechanisms to improve access to affordable devices and through enhancing the enabling environment for e-commerce to support Kenya's role as a regional digital hub.

1.4 Component 4. Project Management- This component will support project implementation, coordination, for the Project Implementation Unit (PIU) within ICTA and capacity building.

1.5 Component 5: Contingent Emergency Response Components-This component will be activated in the event of an emergency.

The GoK intends to apply a portion of the proceeds of the Credit to cover Information Security activities under Component 1 (Digital Infrastructure and Access), Component 2 (Digital Government and Services) and Component 3 (Digital Skills and Markets) .The project aims to accelerate digital transformation at the regional level focusing on critical digital enablers that 'future-proof' economic growth and leveraging Kenya's leadership role in the region to facilitate the adoption and implementation of regionally harmonized frameworks for digital integration.

2. Objectives of the Assignment

The Information Communication Technology Authority (ICTA) is looking to hire an individual Consultant (Digital Information Security Expert) who will work with the

[1] The Program Information Document for KDEAP, and other documentation, is available at: https://projects.worldbank.org/en/projects-operations/project-detail/P170941.

Project Implementation Unit (PIU) and will be responsible for undertaking all Information Security activities for One Government Network/Architecture.

3. Scope of Services and specific tasks of the Assignment

3.1 Scope of services

The Digital information Security Expert will proactively work on the development of base registries and core reusable architectural building block components for a One-Government Experience as per: 1) the Kenya National Digital Master Plan 2022-2032, 2) the Kenya Government Digital Architecture Strategy 2023 and 3) the KDEAP Project implementation components.

Specifically, the Expert will:

1) Work collaboratively with the Ministry responsible for ICT and the Digital Economy, ICTA and other experts on the development and implementation of an enterprise architecture for the GoK to ensure information security is a core element in all aspects of the enterprise architecture.
2) Provide advisory expertise in the area of information security policy for digital transformation, particularly as it relates to enterprise architecture, data protection, privacy, interoperability, etc.
3) Provide hands-on support interventions for information security.
4) Develop standards and guidelines for information security for the GoK.
5) Develop set of best practices, policies, tools, and security protocols designed to help secure GoK digital infrastructure at all level.

3.2 Specific tasks of the assignment

The Consultant will perform the following tasks:

i. **Enterprise Architecture Tasks**

The consultant will perform the following:

Work to refine and deepen the One-Government Experience enterprise architecture vision currently elaborated by the GoK to prepare for implementation specifically with respect to information security.

Advise and develop, in collaboration with the Ministry responsible for ICT and the Digital Economy, ICTA and other experts, the business, information systems (data and applications) and technology architectures for the One-Government Experience Vision.

Assist ICTA and its parent Ministry in developing a future-state government architecture target and work with other experts to develop a roadmap of how to achieve this architecture.

Assist ICTA and its parent ministry in developing governance structures for the implementation of an enterprise architecture.

Working collaboratively with MICDE, ICTA and other experts, develop a broad and overarching governance structure that will assist the GoK to plan, manage and effectively sustain the enterprise architecture in the future.

ii. Cyber-Resilience Plan

Develop a cyber-resilience plan that will permit the GoK to: 1) anticipate (maintain a state of informed preparedness) threat events, 2) respond and withstand (continue with essential functions despite the adversary) threat events, 3) recover (restore essential functions despite adversity) from disruption, and 4) adapt (modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments) from threat events.

As part of the cyber-resilience plan, perform a risk assessment of the GoK. This assessment shall help the GoK understand, characterize and communicate the risk they face from all types of threats. It will, at minimum include: 1) threat characterization, 2) delineation of mission essential functions, and 3) a business impact analysis that helps the GoK: a) determine mission critical processes and their recovery criticality, b) identify resource requirements and c) identify recovery priorities.

As part of the cyber-resilience plan, develop contingencies strategies that will strengthen the GoK ability to anticipate threats and reduce risk by mitigating vulnerabilities, i.e. reducing the GoK attack surface.

As part of the cyber-resilience plan, develop a plan that will permit the GoK to respond to disruptions. This shall include identifying leadership resources, activation and notification phases, damage assessment, recovery and reconstitution phases.

As part of the cyber-resilience plan, develop a strategy for the implementation and continued maintenance of the plan. This shall include policies and procedures that trigger such reviews.

As part of the cyber-resilience plan, develop a test, train and exercise strategy that permits the GoK to maintain its readiness posture. Exercise shall include both functional and tabletop form.

iii. Security Operations Center

Hands-on assistance providing support to the GoK Security Operations Centre including development of policy and guidelines, best practice configuration, etc.

iv. Security Policy

Develop Information Security policy governing access control, acceptable use, data protection, data classification, mobile devices, encryption, intrusion detection, etc.

Provide a set of best practices, policies, tools, and security protocols designed to help secure GoK data and service operations

4. Duration and Location of Assignment

The assignment will be an overall period of thirty-six (36) calendar Months. It is intended that this Consultant will be contracted for a period of twelve (12) calendar Months from the date of commencement with a probation period of three (3) calendar months. This contract period is subject to extension for a further twenty-four (24) calendar months based on satisfactory performance, project funding and project needs.

The Digital Information Security Expert shall be based in ICT Authority, 12th floor Telposta Towers, Nairobi, Kenya with travels as required country-wide to review the project progress.

5. Reporting Requirements and Timeline for Deliverables:

The Digital Information Security Expert will prepare a monthly report highlighting the tasks performed, challenges, and specific recommendations on key actions that should be taken to steer the project to success. All reports prepared by the Digital Information Security Expert shall be reviewed and submitted to the Project Coordinator.

All reports will be submitted within 7 days after the end of reporting month or period in hard and soft copies (in Microsoft Word, Excel, or Power Point, or in any other format as may be deemed appropriate by the PIU Project Coordinator. These reports will accompany the consultant's timesheet for payment.

6. Payment Schedule/Remuneration

The Digital Information Security Expert shall be remunerated based on a consolidated monthly rate (inclusive of all tax obligations), which will be negotiated with the successful candidate during Negotiations. Remuneration will be based on competitive rates, commensurate with the selected candidate's area of expertise and work experience, provided he or she has satisfactorily fulfilled all requirements stipulated herein above.

Payment shall be monthly upon submission and approval of the monthly reports. The consultant will submit to the Project Coordinator, a monthly timesheet, with a supporting invoice, as the basis for payment for the consultancy services. Costs incurred by the Digital Information Security Expert outside the assignment location will be reimbursed upon submission of a statement of expense and verifiable supporting documentation to the KDEAP Project Coordinator.

7. Minimum qualification and experience requirements

The Consultant shall possess the following minimum qualifications and experience:

I. A minimum of a Master's degree in Management Information Systems, Telecommunication Engineering, Computer Science or related field from an institution/university recognized in Kenya.

II. A minimum of 7 years of general work experience.

III. A minimum of 10 years specific experience in Information Security, risk, compliance and policy development and General knowledge of Information Security regulatory requirements and standards such as ISO 27001.

IV. Must have relevant professional certifications in information systems security such as CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), ISO/IEC 27001 Lead Auditor or equivalent.

8. Management and Accountability of the Assignment

The Client for the services will be ICTA. The Client will be represented by the Chief Executive Officer (CEO). The Project Coordinator will be the Consultants' supervisor, and shall be responsible for coordination of activities of the consultant. On a day-to-day work basis, the consultants shall work and report to the Project Coordinator.

9. Responsibility of the Client

The consultant shall be contracted by the ICTA. The consultant must ensure that the tasks identified above are performed in a result-oriented manner with the sole objective of achieving outputs and outcomes expected from the assignment as has been described in the details above. The consultancy is encouraged to utilize local expertise as appropriate.

The client will provide free of charge all available existing information including the communication strategy, data, reports and clips and will assist the Consultant in obtaining other relevant information and materials from governmental institutions and state authorities where necessary. However, it is the duty of the Consultant to check availability, quality and suitability of this information. The information, data, reports as mentioned above will be available for the consultants unlimited use during execution of the proposed services within the project.

Where travelling individually on project duties, subsistence allowance shall be paid in the equivalence of the Public Service Job Group P rates. All individual travel shall be approved prior to the task by the Project Coordinator.

10. Responsibilities of the Consultants

The Consultant shall be responsible for their own transport, accommodation, insurance, Airtime and other associated costs.

The Consultant is expected to undertake activities that will ensure that outputs are consistent with the professional and legal requirements. All outputs will be presented using modern techniques/technology and will form part of the digital land information systems for informal settlements being generated by the Project. It is also required that the data is generated through a consultative process that guarantees authenticity and ownership.

11.0 Confidentiality, Propriety Rights of Client in Reports and Records.

All the reports, data, and information developed, collected, or obtained during performance of the contract from the client or other Institutions shall belong to the Client. No use shall be made of them without prior written authorization from the Client.

At the end of the Services, the Consultant shall relinquish all data, manuals, reports and information (including the database, codes, and related documentation) to the Client and shall make no use of them in any other assignment without prior written authority from the Client.