NATIONAL INFORMATION TECHNOLOGY AUTHORITY-UGANDA

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES TO DEVELOP THE NATIONAL CYBERSECURITY INSTITUTIONAL, GOVERNANCE AND COORDINATION STRUCTURE

OCTOBER 2023

1. INTRODUCTION AND BACKGROUND

The NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NITA-U), (herein after called "the CLIENT") is an autonomous agency of the Government of Uganda established by the National Information Technology Authority, Uganda Act, 2009 to coordinate, promote and monitor Information Technology (IT) developments in Uganda within the context of National Social and Economic development.

The Government of Uganda, through the National Information Technology Authority, Uganda (NITA-U) has received funding from the World Bank/IDA towards financing the Uganda Digital Acceleration Project – Government Network (UDAP-GovNet). The National Information Technology Authority of Uganda (NITA-U) is the Lead Implementing Agency for this Project. As part of UDAP-GovNet, the goal is to transform the way people, governments, businesses and civil society interact with each other, by supporting digital transactions and e-services that can be delivered in a paperless, cashless and secure manner without the requirement for in-person interaction, which in turn also contributes to climate mitigation. The Government of Uganda (GoU) regards cybersecurity as an enabler of efficient, effective, safe and secure delivery of crucial public services. Cybersecurity also serves broader national security goals by protecting Critical Information Infrastructure.

In line with the above, GoU developed the National Cybersecurity Strategy in 2022 that provides the development paths, policy and technical recommendations for the country's increased cybersecurity maturity. The Strategy includes a provision to formulate an institutional framework for cybersecurity governance that identifies the key national players and their roles. There is need to move to the next step of defining the finer details of national-level coordination in cybersecurity in order to progress on the implementation of the strategy. In order to address this need, NITA-U seeks to procure a Firm under contract to develop the National Cybersecurity Institutional and Governance Coordination Structure for Government of Uganda.

2. SCOPE OF CONSULTANCY SERVICES

The Consulting Firm shall be required to interact with /stakeholders in the National Information Security Advisory Group. The number of stakeholders will not exceed 25 and any other relevant stakeholders deemed necessary to provide vital input into the work. National Information Technology Authority – Uganda is the lead agency and coordinator for this assignment. This work is wholly civilian in nature and does not include support for military, intelligence or public security activities.

The assignment will focus on the following:

a) Conduct an independent situational analysis of the existing cybersecurity institutional, governance and coordination practices among public sector agencies
b) Conduct a benchmark to identify practical best practices that support effective and efficient cybersecurity institutional, governance and coordination among public sector agencies and line ministries
c) Develop the proposed National Cybersecurity Coordination Structure for Government of Uganda based on the items (a) and (b) above
d) Deliver validation workshops for the proposed National Cybersecurity Coordination Structure.

3.0 KEY DELIVERABLES AND REPORTING

The expected deliverables for this assignment are detailed below. The deliverables/outputs Reports shall be submitted in paper (2 hard copies each – signed original and duplicate) and electronic format. The Consulting Firm shall be required to submit electronic reports in MS Word, pdf files (secured) and presentations in MS Power Point. Reports will be submitted in English only.

3.1 Task 1: Inception Stage

Upon signing the contract, the Consultant shall be availed with information and other supporting materials that provide background data (as indicated in section 7 below) to support in the development of the Inception Report. This report will contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines subject to NITA-U's approval.

Task 1 Deliverable:
The Consultant shall submit an Inception Report from Task 1.

3.2 Task 2: Conduct an independent situational analysis

The Consultant shall conduct an in-country independent situational analysis of the existing cybersecurity coordination practices between twelve (12) public agencies. NITA-U will provide the identification of the key actors and facilitate introductions to the Consulting Firm. The analysis should assess the current level of inter-agency cooperation and adequacy of cybersecurity coordination. The Consultant shall convene an in-country meeting with NITA-U to review the result of task 2.

Task 2 Deliverable:
The Consultant shall submit the report from the independent situational analysis from task 2.

3.3 Task 3: Conduct an international benchmark study

The consultant shall conduct an international benchmark study to identify practical best practices that are applicable to the Ugandan context. The purpose of this task is to identify viable best practices and lessons learned in achieving a state of efficient and effective national cybersecurity institutional and governance framework and coordination. The Consulting Firm shall propose five countries/ regional blocks for approval by NITA-U before initiation the benchmark. In addition, the parameters of the benchmark will be prior approved by NITA-U. The Consultant shall convene a meeting with NITA-U to review the result of task 3.

Task 3 Deliverable:
The Consultant shall submit the international benchmark report from Task 3.

3.4 Task 4: Develop the National Cybersecurity Coordination Structure

The Consultant shall develop the proposed National Cybersecurity Institutional, Governance and Coordination Structure for Government of Uganda, taking into consideration the goals of the national cybersecurity strategy and the findings from the tasks above. The aim is to improve

awareness of cybersecurity coordination in the various national settings, support the country in enhancing its operational cybersecurity governance, encourage the spread of best practice and contribute to the development of inter-agency and international cooperation. It should further focus on guidelines for the institutions and governance of operational cybersecurity capabilities, cyber incident management and cyber aspects of crisis prevention and management. The coordination structure must at the minimum address the following:

a) Inter-agency coordination structure
b) Inter-agency information sharing
c) Governing rules
d) Code of conduct
e) Information Exchange Protocols
f) Standard Operating Procedures
g) National Cyber Crisis warning tiered levels
h) Informal Rules
i) Promoting and Maintaining Trust
j) Responsible Disclosure
k) Feedback and continuous imrpovement

The Consultant shall convene an in-country meeting with NITA-U to review the result of task 4.

Task 4 Deliverable:
The Consultant shall submit the National Cybersecurity Coordination Structure from Task 4.

3.5 Task 5: Validation for the National Cybersecurity Coordination Structure

The Consultant shall design, plan and execute the validation and sensitization of three (3) in-country workshops for the National Cybersecurity Coordination Structure. NITA-U shall lead the identification and coordination for the participants of these workshops. These shall cover:

a) Political and Policy decision making level
b) Top Management and Executive level
c) Technical and Operational level.

Task 5 Deliverable:
The Consultant shall submit the report from Task 5.

3.7 Task 6: Final Report

The Consultant shall prepare and deliver to the NITA-U a substantive and comprehensive final report of all work performed under these Terms of Reference.

Task 6 Deliverable:
The Consultant shall provide a Final Report from this assignment.

Table 1: Deliverables and submission Timelines

No.	Name of Deliverable	Contents of deliverable	Timeline for each deliverable
1	Inception Report	This report will contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines	**0.75 months**
2	Report from the independent situational analysis	All works related to this deliverable	**1 month**
3	International benchmark report	All works related to this deliverable	**1 month**
4	The National Cybersecurity Coordination Structure	All works related to this deliverable	**2 months**
5	National Cybersecurity Coordination Structure Validation	Validation results, findings and report	**1.1 months**
6	Final Report	Executive summary, the key findings, providing all of the findings, analysis and deliverables	**0.75 months**

4.0 MINUMUM REQUIREMENTS OF THE CONSULTING FIRM AND KEY STAFF

4.1 Requirements for the Consulting Firm

a) Shall be legally registered in Uganda or abroad.
b) The firm must demonstrate previous experience in information security consulting and advisory. The firm should be able to demonstrate their ability to develop and tailor national level cybersecurity frameworks to specific target audiences and industries in at least 5 (five) assignments of similar type, scope and nature. Consulting firms should present documentary evidence details of these similar assignments and must include at the minimum signed letters of completion from the clients, scope and proof of certification (including start and finish dates).
c) The firm should demonstrate experience in advisory related to National Computer Emergency Response Team (CERT) operations. Consulting firms should present documentary evidence details of at least one (1) similar assignment and must include

at the minimum signed letters of completion from the clients, scope and proof of certification (including start and finish dates).

d) The consulting firm must demonstrate ability to field a team of experts with required qualifications and experience for the assignment. The team of experts should include local experts due to the heavy workload in-country and nature of assignment (Must present profile for each required expert with mandatory documentation including CV, copies of required certifications and qualifications as well as a section showing the required experience)
e) Consulting Firms may associate with other firms of a Joint Venture (JV) or a sub consultancy to enhance their qualifications.

The Consulting Firm is required to elaborate in their proposal the envisaged logistical set-up and deployment of appropriate skills for the execution of the assignment. The consultant should carefully review the scope of work and propose a team of well-organized competent staff, adequately equipped with the necessary skills/facilities to execute the assignment, bearing in mind that a substantial amount of work in this assignment is field based in country.

4.2 Expertise and Qualifications of Team Members

The consulting firm should field a team of key experts and non-key experts including among others the following key experts.

4.2.1 Team Leader (1)

Roles and Responsibilities

i. Responsible for the overall management of the assignment and successful timely completion of all deliverables
ii. Ensures the quality of all deliverables by providing guidance and coordinating with team members with their inputs and contribution.

Experience

i. The consultant should have at least fifteen (15) years of experience working on ICT and cybersecurity consultancies, projects with documented experience on leading teams. This must be clearly documented on the CV
ii. Have led at least three (3) projects having similar objectives
iii. The consultant should have a profound theoretical as well as practical knowledge and experience in the relevant fields.
iv. The consultant should have good skills in strategic planning, policy level document development.
v. Excellent written and verbal communication skills.
vi. Excellent planning skills
vii. Fluent oral and written English language skills

Qualifications

i. The consultant should have a Masters's Degree in Information Technology, ICT Management, Information Security or related areas from an internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal
ii. Bachelor's degree in Information Technology, ICT Management, Information Security
iii. or related areas from an internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal.
iv. Certification in any of the following: CISSP/CISA/CISM
v. Project Management certification: Prince 2/PMP

4.2.2 Cybersecurity Experts (3)

Roles and Responsibilities

i. Responsible for the cybersecurity input for tasks 2,3,4 and 5
ii. Participating and leading in the validation meetings.

Experience

i. The consultant should have at least five (5) years of experience working on ICT and cybersecurity consultancies, projects with documented experience. This must be clearly documented on the CV
ii. The consultant should have a profound theoretical as well as practical knowledge and experience in cybersecurity
iii. Fluent oral and written English language skills

Qualifications

vi. The consultant should have a Bachelor's degree in Information Technology, ICT Management or related areas from internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal.
vii. Any of the following industry certifications: CISSP/OSCP/CISM/CEH. Copies of these valid certifications must be provided within the Firm's proposal.

5.0 DURATION OF ASSIGNMENT

The assignment is scheduled for a total of 6.6 months from the date of contract effectiveness.

6.0 REPORTING

The selected consulting firm shall report to the Director Information Security or any persons that may be selected by the Director Information Security. In addition, the consultant shall be required to provide a weekly and monthly report detailing progress achieved and/or any difficulties encountered prior to providing the final project report. Further information can be obtained at the address below during office hours from 08:00 to 17:00 hours East African Time (EAT) on working days and from the NITA-U website (http://www.nita.go.ug)

7.0 DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

The Client will provide the following information, data or reports:

a) National Information Security Framework
b) National Cybersecurity Strategy

8.0 REQUIREMENT FOR QUALITY PLANS

The Consulting Firm will be required to demonstrate in their proposal, evidence of adoption of use of a Quality Assurance System as well as to describe how quality control will be implemented in the course of the assignment.

9.0 PAYMENT SCHEDULE

No.	Description	Percentage
1	After acceptance of the Inception Report	10%
2	Detailed report from the independent situational analysis	20%
3	International benchmark report	15%
4	The National Cybersecurity Coordination Structure	20%
5	National Cybersecurity Coordination Structure Validation results, findings and report	30%
6	After acceptance of the Final Report	05%
Total		100%