MINISTRY OF INFORMATION AND COMMUNICATIONS

REPUBLIC OF SIERRA LEONE

SIERRA LEONE DIGITAL TRANSFORMATION PROJECT
IDA- E1130-SL

Terms of Reference
for

TECHNICAL ASSISTANCE FOR DEVELOPMENT OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION PLAN/GUIDELINES AND PILOTING THE APPLICATION OF THE CIIP PLAN TO FOUR (4) SELECTED SECTORS

[1.4.4]

June 2024

Terms of Reference

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION PLAN

I. Introduction

The Government of Sierra Leone (GoSL) has committed to transforming its economy based on a more inclusive and human-centric digital growth and development approach. A high-level vision for the digital economy is articulated in the new National Digital Development Policy (NDDP), which was approved by the Cabinet in December 2021, setting the GoSL's vision to transform Sierra Leone into an inclusive digital economy and society and to leverage digital technology to support the GoSL to deliver on its national development plan effectively and efficiently. The Sierra Leone Digital Transformation Project (SLDTP) aims to expand access to broadband internet, increase digital skills and improve government capacity to deliver public services digitally. The Project will support the development of a robust enabling environment for the Nation's digital transformation and digital development agenda as articulated in the National Digital Development Strategy.

II. Project Description

The Sierra Leone Digital Transformation Project (SLDTP) is a five-year International Development Association (IDA)-funded Project supported by a US$50 million grant. The Project's primary implementing agency is the Ministry of Communications, Technology and Innovation (MoCTI). The proposed Project Development Objective (PDO) is to expand access to broadband internet, enhance digital skills and improve government capacity to deliver public services digitally.

The SLDTP proposes four integrated and mutually reinforcing components, with a fifth component dedicated to contingent response to future emergencies (*Contingent Emergency Response Component*, *CERC)*.

- Component 1 – Expanding Digital Access and Increasing Resilience of the Digital Environment
- Component 2 – Digital Skills Development and Innovation
- Component 3 - Laying Key Foundations for Digital Government Services and Systems
- Component 4 – Project Management and Implementation Support and
- Component 5 - Contingency Emergency Response Component (CERC).

The proposed activities integrated into Components 1, 2, and 3 are designed to support the Government in building resilient and inclusive policies by strengthening its legal and regulatory frameworks, scaling up the citizen-centric digital public service delivery by reinforcing the government portal and relevant Ministries, Departments, and Agencies (MDAs) capacity. By enhancing the service delivery infrastructure and platforms, the Project will support and ensure the continuity of public services in times of crisis. The Project is being implemented by a Project Coordination Unit (PCU) in the MoCTI.

As Sierra Leone embarks on this digital transformation journey, there is a need to build the capacity of the government, the private sector and the general population more broadly to effectively manage associated cybersecurity risks. Thus, the Government's vision for cybersecurity is to have an enabling environment that is secure, credible, and trustworthy for using ICTs while empowering citizens with the freedom to use the Internet safely for the Nation's socio-economic benefits. This responsibility lies directly within the scope of Component One in the SLDTP project, which aims to enhance digital access and bolster the resilience of the digital environment.

The Technical Leading Agency (TLA) for Cybersecurity for the Project is the National Cybersecurity Coordination Centre (NC3). NC3 is a sub-vented Agency established by the Cybersecurity and Crime Act 2021. This institution oversees all cybersecurity issues in Sierra Leone, including providing support to computer systems and networks in preventing and combating cybercrimes in Sierra Leone, formulating and implementing national cybersecurity policy and strategy, overseeing the management of computer forensic laboratories, providing support to the Judiciary and other law enforcement agencies in the discharge of their functions concerning cybercrime in Sierra Leone, promoting Sierra Leone's involvement in international cybersecurity cooperation and doing other acts or things that are necessary for the adequate performance of the functions of the relevant security and enforcement agencies under the Act.

III. Objectives

a. General Objectives

The SLDTP is seeking the services of a qualified firm to develop a robust national cybersecurity risk management framework for the protection of all critical information infrastructure (CII) whose compromise by a cyberattack can have a debilitating impact on national security, provision of essential services, the economy and public safety. This framework will include i) the identification of sectors to be considered as Critical Infrastructure (CI), ii) the main stakeholders/operators in these sectors, and iii) the digital systems that should be considered CIIs, as well as the development of Critical Information Infrastructure Protection (CIIP) plans at the national and sectoral levels.

b. Specific Objectives

More specifically, the purpose of this assignment is to:

- Ascertain the availability, integrity, confidentiality and resilience of the CII systems that underpin the Nation's ability to function and deliver essential services.

- Enhance the security posture of operators to protect against cyber threats that could compromise national security and adversely affect the country's economic conditions.

- Protect sensitive and confidential information critical information infrastructure sectors hold, including personal data, financial records, and classified information.

- Establish measures and procedures to maintain the continuous operation of critical information infrastructure in the face of cyber incidents, ensuring minimal disruption to essential services.

- Leverage international cybersecurity standards and best practices for CIIP, including NIS2 directive in the EU and CISA's policy initiatives in the US.

- Establish effective incident response mechanisms to detect, analyze, and mitigate cyber incidents promptly, minimizing their impact on critical infrastructure.

- Foster collaboration between government entities and private sector organizations that operate critical infrastructure to increase the protection of CIIs, manage risks and encourage the sharing of information and resources.

IV. Scope of Assignment

The Consultant (Firm) will adopt a multi-pronged approach to developing Sierra Leone's cybersecurity risk management framework for CIIP, and focus initially on four (4) critical sectors, to be determined by the GoSL:

- The first aspect will support the development of a National Critical Information Infrastructure Protection Plan (NCIIPP), which will identify CI sectors, including selecting/identifying a coordinator for each CI sector, whether within NC3, within a Government Ministry, Department or Agency (MDA), or in the private sector, as the lead for each sector.

- The second aspect will focus on identifying the essential entities within each CI sector, including defining the criteria for designating CI operators, defining clear roles and responsibilities of CI operators and stakeholders.

- The third step will be to identifying within each CI operator the essential digital systems (CII).

- The fourth step will be to develop sector-specific CIIP plans for the priority sectors, including developing risk registries, disaster recovery plans, incident response capabilities and standard operating procedures (SOPs), and defining minimum cybersecurity requirements for the CII of CI operators, including processes (e.g., vulnerability management, personnel trainings), technical mitigations (e.g., multi-factor authentication, encryption), and specific standards for CII sector/systems to consider.

- The fifth step will be to evaluate current capacity and monitor progress through regular audits, cyber drills, tabletop exercises, etc.

To meet these objectives, the Consultant (Firm) will undertake the following tasks:

1. **Inception Report (Deliverable 1)**

   a. Review, familiarize and assess the existing risk environment affecting critical information infrastructure (CII) in Sierra Leone, considering the general socio-economic conditions, policy, legal and regulatory frameworks, operating environment, and private and public sector collaboration, thus creating a current state profile.

   b. Analyze existing CII risk management frameworks (e.g. NIST, NIS2, CISA's publications) and compare/contrast the strengths and weaknesses of each framework to evaluate the overarching framework to adopt for the assignment (Deliverable 2)

   c. Define and outline the methodology and approach to be used in the development of the national information infrastructure protection plan (Deliverable 2)

2. **National Information Infrastructure Protection Plan – NIIPP (Deliverable 2)**

   a. Conduct a stakeholder analysis to identify and engage all the Government, private sector (CII Operators, hard and software vendors operating in the country), academia and other relevant entities required for the assignment and determine their interests, expectations, and contributions.

   b. Using a multi-stakeholder approach:

      i. Develop and clearly define criteria and methods to systematically identify and designate CII sectors, operators, and systems/services.

      ii. Conduct a comprehensive assessment to determine dependencies and identify the CII sectors and services in Sierra Leone.

      iii. Develop a strategic direction to build and sustain the security and resilience of the country's CIIs couched in a vision, mission and strategic goals. The goals should be augmented by key priorities that will be implemented within 5 years to improve the Nation's CII resilience and maturity level.

      iv. Develop clear roles and responsibilities of critical infrastructure partners that will give rise to a proactive and inclusive partnership among all levels of Government and the private and non-profit sectors and consequently provide optimal critical infrastructure security and resilience.

c. Develop the NIIPP using a risk-based approach that will serve as the national framework used to protect or preserve all critical information infrastructure and essential services for all sectors of activities. It should identify a Government Ministry, Department or Agency (MDA) as the coordinating lead for each industry, define the criteria for assigning and designating CIIs, define clear roles, responsibilities and capabilities of CII partners and stakeholders and set out processes, requirements, and specific standards ***(as required in Part III, Section 7, subsection 2 of the Cybersecurity and Crime Act of 2021)*** for CII sectors to consider when devising their sector-specific plan. The plan should provide strategic direction for the national effort. It should include managing the risks from significant threats and hazards to physical and cyber critical infrastructure, requiring an integrated approach across state-driven and operator-driven combinations.

3. Identification of CI Operators and essential digital systems (CII) (Deliverable 3)

a. Using the criteria developed in Deliverable 2, conduct a comprehensive assessment of the CII sectors to identify all key systems and assets that are critical for the sector's functioning and delivery of essential services.

b. Map the dependencies between different sectors and systems and identify systems that are critical not only within their own sector but also those that have cascading effects on other sectors. Also take into consideration cross-border dependencies.

c. Using the criteria developed in Deliverable 2, identify all the CII operators in the country.

4. Development of Sector-Specific CIIP Plans for Four (4) Priority Sectors (Deliverable 4)

a. Propose the four priority sectors and identify and engage key stakeholders within the specific sectors, including government agencies, industry associations, regulatory bodies, and private sector organisations.

b. Review existing regulations and legal frameworks related to the sector to identify gaps with emerging international best practices (e.g., NIS2). .

c. Conduct a comprehensive assessment specific to the sector using toolkit such as the NCRA model considering industry-specific threats, vulnerabilities and risks and potential impacts.

d. Develop for each sector a set of baseline cybersecurity requirements, including processes and technical mitigations such as vulnerability management, personnel training plans, use of MFA and encryption, etc.

e. Based on the result of the sector risk assessment, develop a risk register that should identify, assess, and manage cybersecurity risks within the sectors.

f. Develop the sector specific CIIP plans for the priority sectors.

5. **Development of Sector-Specific CIIP Plans for four (4) Priority Sectors (Deliverable 5)**

a. Propose a framework to regularly monitor progress in the priority sectors, for instance through cyber drills, tabletop exercises and audits.

V. Reporting, Time Schedules, and Payment Schedule

The Consultant is expected to complete the assignment in full within 12 months. The Consultant will regularly report to the National Cybersecurity Coordinator on all aspects of the agreed activities and also report to the SLDTP Project Coordinator.

The deliverables comprise the following:

No	**Deliverable**	**Timeline**	**Indicative payment schedule**
1	Inception Report	Commencement + 1 month	10%
2	National Information Infrastructure Protection Plan – NIIPP	Commencement + 4 months	20%
3.	Identification of CI Operators and CII Systems in four (4) sectors	Commencement + 8 months	25%
34	Development of Sector-Specific CIIP Plans for four (4) Priority Sectors	Commencement + 12 months	20%

VI. Qualification and Experience of Consultant

The assignment calls for a team of at least 5 personnel who will possess the following qualifications, skills, and experience:

Key Position	Experience	Qualifications
(1) CIIP Lead / Cybersecurity Expert	Min. 10 years' experience in cybersecurity, cyber operations, cyber defense, cyber threat investigation (CTI), and digital development, part of which must have been spent on developing CIIP strategy and implementation plan. 5 years or more of experience in implementing donor-funded programs as a Team Leader or equivalent. Networks and relationships with governmental and/or private sector entities in Sierra Leone is preferable.	Master's degree in cybersecurity Information Security, or other relevant fields.
(1) Information Security Expert	Min. 5 years' experience in IS management supported experience in working in CIIP projects or related assignments.	Master's degree in information security, computer technology, information systems, or a related field. A bachelor's degree in addition to experience implementing CIIP programs combined with relevant industry certifications will be considered.
(1) Cyber Risk Management Expert	Min. 5 years' experience in cyber risk management, cyber operations, cyber defense and cyber threat investigation (CTI). Experience in risk assessment and compliance monitoring, business impact analyses, threat analysis, risk management, cybersecurity policy and governance or related job roles.	Master's degree in Cybersecurity, Information Assurance, Risk Management or related field
(1) Business Continuity Expert	Min 5 years' experience in developing business continuity plans and implementing key deliverables in risk management profiles.	Bachelor's degree in Business Administration or related field plus min. 3 years of experience in Business Continuity. Knowledge of Business Continuity principles and frameworks and

	Experience in maintaining business's level of readiness to restore critical functions after an emergency or disruption.	familiarity with risk management techniques
(1) Communications Expert	Min. 5-year experience in creating, implementing and oversight of communications programs, promoting project objectives and ideals. Experience in working with professionals, departments, senior management, and members of the media and press.	Bachelor's degree in communications, journalism, business, advertising, English, or Public Relations

VII. Facilities Data and Information to Be Provided by Client

For the execution of the assignment, the National Cybersecurity Coordinator will provide necessary documentation in its possession relevant to the execution of the assignment.