

MINISTRY OF COMMUNICATION, TECHNOLOGY AND INNOVATION



REPUBLIC OF SIERRA LEONE

SIERRA LEONE DIGITAL TRANSFORMATION PROJECT

IDA- E1130-SL

Terms of Reference

for

**The Recruitment of an Individual Consultant for the Review for the Cybersecurity and
Crime Act 2021 and Development of Governance and Regulatory Framework**

SL-MoF-565256-CS-INDV

August 2026

Terms of Reference

Recruitment of a Consultant for the Review for the Cybersecurity and Crime Act 2021 and Development of Governance and Regulatory Framework

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 strong 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)

The Sierra Leone Digital Transformation Project (SLDTP) is a five-year International Development Association (IDA)-funded project supported with a US\$50 million grant. The project's main implementing agency is the Ministry of Communication, 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 ensuring the continuity of public services in times of crisis.

The Project is being implemented by a Project Coordination Unit (PCU) in the MoCTI. The MoCTI is the primary stakeholder of ICT-related policies and is tasked with overseeing the development, review, and implementation of the Government's Technology, Communications and Innovation agenda. The MoCTI facilitates universal, ubiquitous, and cost-effective access to information and communications infrastructure and services throughout the country. Digital infrastructure provides a way for people, businesses, and governments to get online and link with local and global digital services, thus connecting them to the global digital economy. Good and affordable internet connectivity is a critical foundation for a digital economy.

III. Project Background

The Government of Sierra Leone (GoSL) has committed to building a secure, resilient, and inclusive digital economy as articulated in the National Digital Development Policy (NDDP) and supported by the Sierra Leone Digital Transformation Project (SLDTP). Digital technologies are now central to public service delivery, economic growth, innovation, and citizen engagement. However, this growing digital footprint has also increased exposure to cybersecurity threats and cyber-enabled crimes.

The Cybersecurity and Cybercrime Act, 2021 (the Act) marked a significant milestone in establishing Sierra Leone's legal and institutional framework for cybersecurity governance, cybercrime prevention, critical information infrastructure protection, and international cooperation. Since its enactment, the national digital ecosystem has evolved rapidly, driven by increased broadband penetration, mobile usage, cloud adoption, digital platforms, artificial intelligence (AI), fintech, e-commerce, and e-government services.

Three years of implementation of the Act, combined with emerging global and regional cyber threat trends, have revealed legal, institutional, and operational gaps that limit the effectiveness of the current framework. These include governance and oversight challenges for the National Cybersecurity Coordination Centre (NCSCC), unclear institutional mandates and coordination mechanisms, limited obligations for digital service providers and platforms, outdated offence typologies and penalties, capacity constraints, and insufficient mechanisms for public-private collaboration.

Cabinet has approved the amendment of the Cybersecurity and Cybercrime Act, 2021 and authorised the Ministry of Communication, Technology and Innovation (MoCTI), in collaboration with the Office of the Attorney General and Minister of Justice, to undertake the necessary reforms. In this context, GoSL, with support from the World Bank through the SLDTP, seeks to recruit a qualified Consultant to conduct a comprehensive assessment of the Act and the broader cybersecurity and cybercrime landscape, and to propose a fit-for-purpose governance, legal, and regulatory framework for the effective management of national cyberspace.

IV. Objectives

General Objective

The overall objective of this assignment is to undertake a comprehensive, evidence-based assessment of the Cybersecurity and Cybercrime Act, 2021 and the evolving national cyber landscape, and to develop a future-ready governance, legal, and regulatory framework that enables effective coordination, enforcement, collaboration, and resilience in Sierra Leone's cyberspace.

The assignment will support the Government to ensure that its cybersecurity and cybercrime framework is coherent, adaptive, enforceable, aligned with international best practices, and responsive to emerging technologies and threats.

Specifically, the consultant will:

- Conduct a thorough legal, regulatory, and institutional assessment of the Cybersecurity and Cybercrime Act, 2021 to determine its adequacy, relevance, effectiveness, and enforceability in addressing current and emerging cyber risks, cyber-enabled crimes, and digital vulnerabilities.
- Evaluate the coherence, alignment, and interoperability of existing policies, regulations, strategies, institutional mandates, and operational arrangements governing cybersecurity,

cybercrime prevention, data protection, digital governance, critical infrastructure protection, and national security.

- Undertake a comprehensive desk review and benchmarking exercise against relevant regional and international legal instruments, frameworks, standards, and best practices, including but not limited to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the Budapest Convention on Cybercrime, ITU Global Cybersecurity Index, NIST Cybersecurity Framework, and ISO/IEC standards, to identify areas of convergence, divergence, and opportunity for reform.
- Identify legal, regulatory, institutional, operational, technical, and capacity gaps, overlaps, inconsistencies, and coordination challenges that may hinder the effective implementation of cybersecurity governance and cybercrime prevention in Sierra Leone.
- Clearly define and rationalise institutional roles, responsibilities, mandates, reporting lines, and coordination mechanisms across Ministries, Departments, and Agencies (MDAs), law enforcement bodies, regulatory institutions, national security agencies, the judiciary, private sector operators, civil society, and development partners, to ensure clarity, accountability, efficiency, and synergy in cyberspace management.
- Design and propose a fit-for-purpose regulatory framework supported by appropriate subsidiary legislation, operational guidelines, compliance mechanisms, and enforcement protocols, ensuring a balanced, risk-based, and proportionate approach to cybersecurity regulation and cybercrime control.
- Develop a comprehensive national cyber governance and coordination framework, including institutional architecture, multi-stakeholder collaboration mechanisms, public-private partnership models, incident response coordination protocols, information-sharing arrangements, and crisis management structures.
- Formulate a clear, actionable, and costed implementation roadmap, including short-, medium-, and long-term actions, institutional capacity-building measures, financing strategies, and sustainability mechanisms.

V. Scope of Assignment

The specific objectives of this consultancy are to:

- Review and assess the effectiveness, adequacy, and relevance of the Cybersecurity and Cybercrime Act, 2021 in addressing current and emerging cyber risks.
- Evaluate existing regulations, policies, institutional arrangements, and operational mechanisms related to cybersecurity and cybercrime.
- Conduct a comprehensive desk review of national, regional, and international legal and regulatory frameworks, standards, and best practices.
- Identify legal, regulatory, institutional, technical, and operational gaps, overlaps, and inconsistencies.
- Clearly define institutional roles, responsibilities, mandates, and coordination mechanisms among key public and private stakeholders.
- Develop a fit-for-purpose regulatory framework and collaborative governance model for effective cyber space management.
- Provide practical implementation roadmaps, operational guidelines, and monitoring frameworks.

Gender and Social Inclusion

The Consultant shall integrate a gender and social inclusion lens throughout the assignment, ensuring that the review of the Cybersecurity and Cybercrime Act, 2021 and the proposed governance and regulatory framework adequately reflect the needs, risks, and vulnerabilities of women, youth, persons with disabilities, and other marginalised groups. This shall include, but not be limited to, the assessment of legal and institutional responses to cyber risks such as online gender-based violence, digital harassment, and exclusion from digital services, as well as the development of inclusive policy, regulatory, and operational recommendations that promote equitable access, protection, and participation in the digital ecosystem.

The Consultant shall undertake the following key tasks:

A. Inception and Planning

- Conduct a project inception meeting with MoCTI and key stakeholders.
- Prepare and submit an Inception Report detailing:
 - Methodology and approach
 - Work plan and timeline
 - Stakeholder engagement strategy
 - Risk management plan

B. Desk Review and Legal & Regulatory Assessment

- Review of the Cybersecurity and Cybercrime Act, 2021.
- Review existing cybersecurity policies, strategies, regulations, and operational guidelines.
- Review related digital laws including data protection, digital government, telecommunications, electronic transactions, critical infrastructure protection, and national security.
- Benchmark Sierra Leone's framework against international best practices, including:
 - African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)
 - Budapest Convention on Cybercrime
 - NIST Cybersecurity Framework
 - ISO/IEC 27001 and 27701
 - ITU Global Cybersecurity Index frameworks

C. Institutional and Stakeholder Mapping

- Identify and map all relevant institutions and stakeholders, including public and private sector players
- Define existing mandates, roles, responsibilities, and coordination mechanisms.

- Identify overlaps, gaps, conflicts, and inefficiencies.

D. Gap Analysis and Risk Assessment

- Conduct a comprehensive gap analysis covering:
 - Legal and regulatory frameworks
 - Institutional
 - Technical and operational

Expected Outcomes:

The outcome of the assignment shall be guided by:

1. Development of Regulatory and Governance Framework

The Consultant shall design a mechanism that will

- Propose amendments on provisions in the current act
- Analysis on Compliance and enforcement mechanisms
- Position cybersecurity as an acceptable global good practice
- Incident reporting and response obligations

2. Governance and Coordination Model

- National cyber governance architecture
- Roles and responsibilities of institutions
- Inter-agency coordination mechanisms
- Public-private partnership model
- International cooperation framework

3. Operational Framework

Assess and proffer advice on efforts of NCCC in relation to:

- Cyber incident response coordination framework
- National CERT/CSIRT operational model
- Information sharing protocols
- Crisis management and escalation procedures

4. Stakeholder Consultations and Validation

- Consult and conduct validation by relevant stakeholders.
- Integrate feedback into final outputs

VI. Key Deliverables and Implementation Timeline

No	Deliverable	Timeline	Indicative Payment Schedule
1	Inception Report and Work Plan	Commencement + 3 weeks	10%
2	Desk Review and Legal Assessment Report	Commencement + 6 weeks	30%
3	Draft Regulatory and Governance Framework	Commencement + 12 weeks	40%
4	Final Report	Commencement + 15 weeks	20%

VII. Qualification and Experience of Consultant

The consultant must have a minimum of eight (8) years' experience in cybersecurity policy, regulation, and governance.

- Proven experience in legal and regulatory reform in the ICT or digital sector.
- Demonstrated expertise in policy and legal drafting
- Strong knowledge of international cybersecurity conventions and standards.
- Experience working with government and development partners on similar assignment
- Familiarity with the Sierra Leonean context or similar settings, particularly around multiple stakeholders, including government ministries, regulatory bodies, civil society, and the private sector, using inclusive and participatory approaches.

VIII. Facilities Data and Information to be Provided by Client

The MoCTI shall provide office space with an Air Conditioner, electricity and Internet connection for the successful Consultant to facilitate the smooth implementation of the assignment. The following shall be provided to the Consultant by the Employer:

- a. Facilitate the provision of access to relevant documents and data available which may be supportive to the Consultant, and
- b. Prepare a letter introducing the Consultant to MDAs and other relevant stakeholders, wherever required in performing the assignment.

The Consultant shall provide all the administrative, technical professional and support staff needed to carry out the assignment efficiently. The Consultant shall also be responsible for providing all other necessary facilities and logistical support for its staff/teams, including accommodation, vehicles/transportation, office equipment, field survey and investigation equipment, laboratory testing, communications, utilities, office supplies and other miscellaneous requirements wherever applicable to render their services. The Consultant shall make himself/herself available for regular meetings with the PCU, NC3 and MoCTI teams.

IX. Working Language

The working language for the consultancy service shall be English.

X. Conflict of Interest

The Consultant must declare any actual, potential, or perceived conflicts of interest that could affect the impartiality of the assignment, including ongoing or recent engagements with telecommunications operators, internet service providers, mobile network operators, digital service providers, or cybersecurity vendors operating in Sierra Leone, as well as any involvement in national cybersecurity systems, CERT/CSIRT services, or digital government platforms under review. This also includes financial, advisory, or employment relationships with regulated entities within the scope of the assignment. The Consultant is required to disclose such relationships at the time of application and throughout the assignment and propose mitigation measures subject to approval by MoCTI and the PCU. Failure to disclose relevant conflicts may result in disqualification or contract termination.

XI. Confidentiality of Information

The Consultant shall protect the confidentiality of the data or information received to conduct this assignment and shall sign a confidentiality agreement with MoCTI. Given the sensitive nature of this assignment, the Consultant shall ensure the secure handling, storage, and transmission of all data and information, including any sensitive or classified government information, and shall take appropriate measures to prevent unauthorized access, disclosure, or misuse.

No data, information, or deliverables from this assignment will be released to third parties without the written approval of MoCTI. All intellectual property rights, including all reports, data, frameworks, and other deliverables produced under this assignment, shall remain the sole property of the Government of Sierra Leone, and the Consultant shall not use or reproduce such materials for purposes outside this assignment without prior written consent.

The Consultant shall surrender all data and other materials to the Regulatory Authority and shall not retain any information or materials after the closure of the assignment. These confidentiality obligations shall survive the completion or termination of the contract.