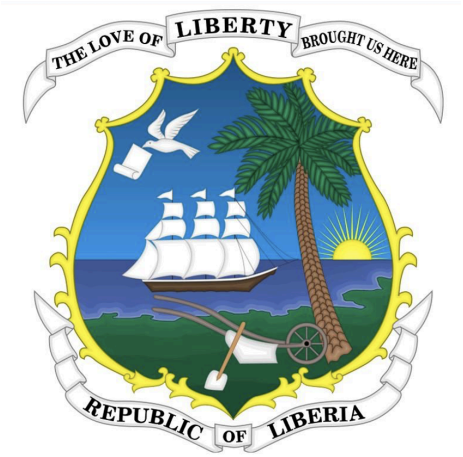

Republic of Liberia

Ministry of Posts & Telecommunications

National Cybersecurity Strategy 2025 - 2029

July 2024

Prepared by SecDev

Under the World Bank contract No 7211387

Comprehensive Assessment of Liberia's Cybersecurity Readiness and Resilience
(The Liberia Digital Transformation Program)

Table of Contents

Abbreviations

CBL	Central Bank of Liberia
CI	Critical Infrastructure
DDoS	Distributed Denial of Service
ECOWAS	Economic Community of West African States
GoL	Government of Liberia
ICT	Information and Communications Technology
IT	Information Technology
LEC	Liberia Electricity Corporation
LREN	Liberia's National Research and Academic Network
LTA	Liberia Telecommunications Authority
MACs	Ministries, Agencies and Commissions
MFDP	Ministry of Finance and Development Planning
M & E	Monitoring and Evaluation
MOPT	Ministry of Posts and Telecommunications
NCA	National Cybersecurity Agency
NCC	National Cybersecurity Council
NCS	National Cybersecurity Strategy
NIST	U.S. National Institute of Standards and Technology
PPP	Public Private Partnership

Foreword

As Liberia embarks on a new chapter, I am pleased to present the National Cybersecurity Strategy, a testament to our commitment to digital transformation and the protection of our nation's digital future. The prioritization of this strategy underscores the vital importance of a secure, reliable, and accessible cyberspace to Liberia's national development, economic growth, and the achievement of sustainable development goals.

Embracing digital technologies is pivotal for driving economic growth, enhancing access to public services, and ensuring a prosperous future for all Liberians. To achieve these goals, it is crucial to have a clear vision, a comprehensive approach, strong policy pillars, and decisive actions to build a trusted and resilient cyberspace.

The National Cybersecurity Strategy is a cornerstone document that articulates Liberia's strategic vision, establishes key objectives, and delineates the pathways for national cybersecurity governance. It aims to safeguard critical infrastructure and promote Liberia's national and societal interests in cyberspace.

This first National Cybersecurity Strategy provides a structured roadmap for achieving these objectives collaboratively over the short, medium, and long term. The strategy's phased approach acknowledges that several objectives will require further adaptation to align with Liberia's National Development Strategy.

Recognizing the dynamic nature of cyberspace, this strategy is designed as a living document. It will be reviewed and updated 24 months and 36 months after its initial adoption to ensure its continued relevance and effectiveness.

The development of the National Cybersecurity Strategy took place between February to June 2024, involving extensive consultations with key actors and stakeholders across Liberia. This collaborative process included Ministries, Agencies and Commissions (MACs), regulators, private sector companies, academic and civil society organizations, and cybersecurity experts. Their collective insights and contributions have been instrumental in formulating a comprehensive strategy that addresses the diverse challenges and opportunities in cybersecurity, ensuring a resilient and secure digital future for Liberia.

As we move forward, this National Cybersecurity Strategy will continue to evolve, adapting to new challenges and technological advancements, to safeguard our nation's digital landscape and secure a prosperous future for all Liberians.

Minister of Post and Telecommunications,
Republic of Liberia

Executive Summary

The National Cybersecurity Strategy (NCS) of Liberia sets forth a comprehensive framework to enhance the nation's cyber resilience, fostering a trusted digital environment. This strategy is designed to address the urgent and evolving cybersecurity needs of Liberia, aligning with the nation's broader development goals.

Strategic Context

Liberia is on a path of digital development, leveraging digital technologies to drive economic growth, enhance public services, and ensure a prosperous future for all. However, this progress is accompanied by increasing cybersecurity risks. Critical service providers in sectors such as energy, telecommunications, transportation, finance and healthcare depend heavily on digital infrastructure, making them vulnerable to cyber threats. The increasing incidence of cyberattacks on government institutions and private companies highlight the urgent need for a structured and strategic approach to cybersecurity.

Approach

The NCS is structured to address immediate and short-term needs from 2024 to 2026, while also laying the groundwork for medium and long-term priorities from 2027 to 2029 and beyond. The strategy is built on three Strategic Pillars:

1. **Build:** Establish an effective governance model and an enabling policy, legal, and regulatory environment.
2. **Protect**: Enhance national incident response capacity, strengthen national cyber readiness, and strengthen operational capacity to combat cybercrime.
3. **Sustain**: Improve national cybersecurity education, promote cybersecurity awareness, and advance international cooperation.

Key Objectives and Actions

- **Establish an Effective Governance Model**: Establishing a National Cybersecurity Council, appointing a National Cybersecurity Coordinator, and developing a strategic roadmap for national cybersecurity governance.
- **Enable Policy, Legal, and Regulatory Environment**: Adopting a National Cybersecurity Act, enacting supporting legislation for data protection and critical infrastructure, and aligning sectoral regulations.

- **National Incident Response Capacity**: Establishing an Incident Response Task Force, formulating a national incident response plan, and conducting national cybersecurity exercises, with the immediate aim of managing critical incidents and the long-term objective of developing a national CSIRT capability.
- **Cyber Readiness**: Preparing a National Cybersecurity Framework and defining baseline cybersecurity measures for public sector and critical infrastructure entities.
- **Combating Cybercrime**: Accelerating the adoption of comprehensive cybercrime legislation, improving technical infrastructure, and enhancing the operational capacity of law enforcement agencies.
- **Cybersecurity Education**: Defining a cybersecurity education framework, integrating cybersecurity into educational curricula, and supporting national cybersecurity research and learning.
- **Cybersecurity Awareness**: Conducting national awareness campaigns, facilitating cross-sectoral collaboration, and publishing awareness-raising materials.
- **International Cooperation**: Aligning national cybersecurity frameworks with regional and global standards, acceding to international conventions, and expanding public communication and engagement.
- **Leverage Regulatory Authority to Create a National Market for Cybersecurity Skills**: Utilize the authority of regulators in critical infrastructure sectors, including banking, energy, and telecommunications, to mandate the maintenance of cybersecurity teams within Liberia. Embed these requirements into licensing conditions to ensure that both private and public sector operators develop and sustain local cybersecurity expertise.

Success Factors

The successful implementation of the NCS and its Action Plan relies on an effective governance model, adequate resources, and a robust monitoring and evaluation framework. The strategy will undergo periodic reviews to ensure its relevance and effectiveness, with the first review scheduled for 2027 and a final review in 2029.

The National Cybersecurity Strategy represents Liberia's commitment to creating a secure and resilient cyberspace, essential for sustainable development and the well-being of all its citizens.

Introduction

In an era where digital technologies permeate every aspect of society, ensuring a secure and resilient cyberspace is paramount for Liberia's national development. The Government of Liberia recognizes that robust cybersecurity is essential not only for safeguarding digital infrastructure but also for promoting economic growth, enhancing public services, and protecting the welfare of its citizens. As Liberia continues its digital development journey, this National Cybersecurity Strategy (NCS) aims to align cybersecurity efforts with national development priorities, accelerating development through practical and sustainable steps.

The NCS of Liberia outlines a comprehensive and strategic approach to creating a secure and trusted digital ecosystem. This foundational blueprint sets forth the vision, objectives, and actions necessary to enhance the nation's cybersecurity posture. It aims to protect critical infrastructure, support economic resilience, and ensure the safety and privacy of all Liberians in the digital realm.

Liberia's commitment to digital development has led to significant advancements in sectors including financial services, healthcare, education, and government services. The rapid expansion of wireless internet connectivity, broadband infrastructure, and mobile phone penetration has created new opportunities for businesses and individuals alike. Mobile money services, for instance, have revolutionized financial inclusion and small business growth, lowering transaction costs and empowering entrepreneurs to access global markets.

However, this digital progress also brings heightened risks. Dependence on digital infrastructure makes critical service providers—such as those in energy, telecommunications, transportation, finance, and healthcare—vulnerable to cyber threats. Cyberattacks on government institutions and private companies have resulted in financial losses, data breaches, and service disruptions, underscoring the urgent need for a coordinated cybersecurity strategy.

Currently, Liberia's cybersecurity governance is in its nascent stages, characterized by fragmented efforts and a lack of centralized authority. To address these challenges, the NCS proposes establishing a National Cybersecurity Council and appointing a National Cybersecurity Coordinator to lead and coordinate national efforts. The strategy also calls for developing a comprehensive legal and regulatory framework, including adopting a National Cybersecurity Act, to provide clear mandates and responsibilities for cybersecurity governance.

A key sustainability component of the NCS is building a national market for cybersecurity skills through the use of regulatory mechanisms and incentives. By leveraging the authority of

regulators in critical infrastructure sectors, including banking, energy, and telecommunications, the strategy mandates the maintenance of cybersecurity teams within Liberia. Embedding these requirements into licensing conditions ensures that both private and public sector operators develop and sustain local cybersecurity expertise. Additionally, incentives such as tax breaks will support education, employment creation and the emergence of a sustainable digital ecosystem.

This first NCS is designed as a living document, adaptable to the evolving cyber landscape. It will be reviewed and updated periodically to ensure its continued relevance and effectiveness. Developed in consultation with a wide range of stakeholders, including state institutions, regulators, private sector companies, academic and civil society organizations, and cybersecurity experts, this strategy reflects a collective commitment to building a secure and resilient digital future for Liberia.

By implementing the NCS, Liberia aims to strengthen its cybersecurity capabilities, protect its digital assets, and foster a culture of cybersecurity awareness and education. This strategy addresses immediate cybersecurity needs and lays the groundwork for sustainable, long-term cyber resilience, ensuring that Liberia can confidently navigate the complexities of the digital age.

Strategic Context

The national cybersecurity priorities outlined in this document are shaped by the unique constraints and opportunities that Liberia faces. This context underscores the urgency and necessity of robust cybersecurity measures.

Impetus for Cybersecurity

Liberia is committed to digital transformation as a pathway to sustainable, inclusive, and growth-oriented development. In recent years, significant progress has been made in establishing a strong foundation for digital development, recognizing its role as a critical enabler of key development milestones. By embracing digital technologies, Liberia aims to improve access to financial services, healthcare, education, and government services for all citizens. This commitment reflects our vision of leveraging technology to drive economic growth, enhance public services, and promote the well-being of every Liberian.

The rapid expansion of wireless internet connectivity, broadband infrastructure, and mobile phone penetration has opened new opportunities for all. This growth empowers small businesses and entrepreneurs to access global markets, driving economic growth and creating employment opportunities. Mobile money services, spearheaded by financial and telecommunications companies, have played a transformative role, enabling financial inclusion, fostering small business growth, and reducing transaction costs across the economy.

The Government of Liberia (GoL) continues to leverage technology to digitize public services and streamline administrative processes, thereby improving transparency, accountability, and reducing corruption. The GoL prioritizes reforms aimed at improving the enabling environment for digital transformation and investments in digital infrastructure. However, this progress comes with elevated risks in cyberspace. Critical service providers in sectors such as energy, telecommunications, transportation, finance and healthcare heavily depend on connectivity, data infrastructure, and underlying technologies. The continuity, quality and growth of services provided by these critical infrastructure providers are at risk. Between 2022 and 2024, several government institutions and leading state and private companies in Liberia experienced significant cyberattacks, resulting in financial losses, leakage of sensitive data and disruption of services.

Moreover, the nation confronts a diverse range of cyber threats, including ransomware, Distributed Denial of Service (DDoS) attacks, botnets, and commodity threats, such as cyber

scams. Cybercriminals increasingly target the online population in Liberia, taking advantage of limited awareness, lower digital and cyber literacy and technical vulnerabilities. These incidents highlight the urgent need for a structured and strategic approach to cybersecurity to protect the emerging digital ecosystem and reinforce trust in the digital transition process.

Liberia must take decisive action to strengthen cybersecurity and safeguard cyberspace for its citizens, businesses, government, academic, and civil society organizations. This strategy addresses these challenges comprehensively and builds a secure and resilient digital future for Liberia.

Cybersecurity Maturity (2024)

An assessment of Liberia's national cybersecurity capacity in early 2024 identified significant gaps, necessitating urgent and comprehensive action across multiple areas.

Liberia's national cybersecurity governance is in its early stages and remains fragmented. There is no centralized national authority or active interagency mechanisms to coordinate cybersecurity efforts across government institutions. Although the Liberia Information and Communications Technology (ICT) Policy (2019-2024) aimed to establish the National Cybersecurity Advisory Committee, progress has been limited. Relevant institutions, such as the Ministry of Post and Telecommunications, the Liberia Telecommunications Authority, Liberia Revenue Agency and the Central Bank of Liberia, have not been leveraged as leaders of nationally significant cybersecurity initiatives.

The existing strategic, policy, legal and regulatory frameworks are outdated and lack specific mandates for institutions to effectively address cybersecurity issues. This gap hinders effective governance and enforcement, leaving the country vulnerable to cyber threats. The absence of specific legislation addressing the cybersecurity of critical infrastructure presents significant risks as it impedes the ability of institutions to proactively manage and mitigate cyber risks. Without clear mandates and updated regulations, coordination among key stakeholders is fragmented, reducing the overall effectiveness of existing cybersecurity efforts. This has been demonstrated by several incidents resulting in service disruptions.

Liberia lacks a cohesive approach to cyber risk management. This is primarily due to missing regulatory incentives and the absence of dedicated cybersecurity institutions. There is no centralized review of risks, comprehensive analysis of the threat landscape, or formal procedures to identify vulnerabilities. Additionally, there is no established system for reporting

vulnerabilities or incidents, nor is there a mechanism for sharing information across sectors. Government institutions have not conducted any cybersecurity readiness exercises, either individually or collectively.

Preparedness and resilience capacity of Liberia remains low to non-existent. National incident response capabilities are inadequate, lacking the necessary structures, such as incident response teams and security operations centers and trained personnel to manage and mitigate cyber incidents effectively. Companies in the telecom, finance, and energy sectors tend to prioritize IT security due to their larger attack surfaces, regional security centers, multi-country standards, and past experiences with incidents.

The existing cybersecurity capacity building, skills development mechanisms in Liberia are in early stages. A systemic approach to developing the country's cybersecurity workforce has been missing, hindered by limited market demand, a small talent pool, and the absence of formal certification and training programs. These issues are further compounded by weak or non-existent regulation of cybersecurity fundamentals. Emerging academic programs designed to train a local cybersecurity workforce require additional investment to reach their full potential and gain market recognition. General awareness building efforts have been sporadic, reaching a small share of Liberians via digital literacy and foundational IT training programs and which are not integrated with national cybersecurity awareness objectives.

While Liberia values international cooperation and participation in global cybersecurity frameworks, existing opportunities have been underutilized. Collaboration to define national cybersecurity frameworks in line with leading regional and global partners has been mostly limited to capacity building and preparatory activities through the Economic Community of West African States (ECOWAS), and International Telecommunication Union (ITU). Liberia has not acceded to such important instruments as the African Union's Malabo Convention, which took effect in June 2023 and the Budapest Convention. Coordinated engagement under bilateral and multilateral cybersecurity initiatives will allow Liberia to benefit from a broader network of cybersecurity expertise, resources, cybersecurity technology, methodologies, and support.

Approach

The National Cybersecurity Strategy of Liberia is designed to build a strong, sustainable foundation for a secure and resilient digital future. This Strategy adopts a pragmatic approach, prioritizing the most critical gaps first to ensure a cohesive and comprehensive cybersecurity framework. The integrated NCS Action Plan within this Strategy is structured in two phases: addressing immediate and short-term needs from 2024-2026 and laying the groundwork for medium and long-term arrangements from 2027-2029 and beyond.

This practical and applied approach ensures that Liberia's cybersecurity agenda is tackled sequentially, from establishing effective national governance, through developing robust policy and regulatory frameworks, to enhancing incident response and recovery capabilities. This strategy aligns with Liberia's broader national development priorities and is designed to make best use of limited resources and human capital, while laying a foundation to expand capacity.

Vision Statement

To establish a strong, sustainable foundation for secure, resilient and trusted digital ecosystems in Liberia, enabling economic growth, ensuring safety, fostering confidence and safeguarding the privacy for all citizens.

This vision emphasizes creating a secure, resilient and sustainable digital ecosystem, reflecting the long-term goals and the five-year planning horizon of the National Cybersecurity Strategy.

Principles

The strategy is founded on a set of core principles that shape its objectives and actions. These principles, endorsed by a wide range of national stakeholders, are the essence of the strategy's practical vision.

1. **Essential for Development**: Addressing Liberia's cybersecurity needs is fundamental for national development and participation in the global economy. The risks posed by cyber threats are significant, and inaction is not an option. The cost of not addressing these threats is too high.

2. **Secure- by-Design Digital Transformation:** Liberia's continued digital transformation has yielded substantial benefits that must be protected. Future digital advancements should be secure-by-design, ensuring that digital systems are protected, safe and trustworthy.
3. **High Return on Investment**: Investments in national and sectoral cybersecurity initiatives offer significant returns. The collective benefits to society and the nation far exceed the sum of resources allocated at institutional, enterprise, or individual levels.
4. **Long-Term, Cooperative Effort**: Cybersecurity is a long-term, shared and cooperative effort requiring cooperation and sound governance. Clearly mandated institutions, effective rules, and tested mechanisms for collaboration, coordination, and incident response are essential.
5. **Whole-of-Government and Whole-of-Society Approach**: National cybersecurity must align with the principles of whole-of-government and whole-of-society. This alignment enables effective coordination, optimal resource utilization, and effective cybersecurity across all layers of government, business, and society.
6. **Sustainable Investments**: Liberia's investments in cybersecurity should be sustainable, leveraging local expertise, skills, and resources. National cybersecurity initiatives should stimulate local market forces, creating incentives for private sector involvement, public-private partnerships, and increased demand for local talent and educational, technical, and advisory services.

Strategic Pillars and Objectives

The National Cybersecurity Strategy (NCS) is built around three strategic pillars, each with specific objectives designed to achieve our overarching goal of a secure and resilient digital ecosystem in Liberia (Table 1). Each objective includes a set of targeted actions to ensure effective implementation and measurable progress.

Table 1. Pillars and Objectives of the NCS

Strategic Pillars	Strategic Objectives
Build.	1.1 Establish an Effective Governance Model 1.2 Enable Policy, Legal and Regulatory Environment

Protect.	2.1 Establish National Incident Response Capacity 2.2 Strengthen National Cyber Readiness 2.3 Strengthen Operational Capacity to Combat Cyber Crime
Sustain.	3.1 Improve National Cybersecurity Education 3.2 Promote National Cybersecurity Awareness 3.3 Advance International Cooperation 3.4 Create a Local Market for Cybersecurity Skills

The objectives and underlying actions are interlinked, each complementing and reinforcing the others. For example, establishing a national cybersecurity governance model alongside legal and regulatory frameworks is essential for developing technical and operational capacities, facilitating the efficient use of limited resources. Investments in cybersecurity education, public awareness, and international cooperation support the success of the governance and regulatory frameworks, and strengthen their long-term sustainability.

Strategic Pillar 1. Build.

The National Cybersecurity Strategy aims to establish the foundational elements necessary for national cybersecurity governance. These elements include mandated institutions and core legal and regulatory frameworks. Without these foundational components, Liberia's gains in other areas of development remain exposed to risks of disruption and loss.

1.1 Establish a Governance Model

Addressing Liberia's national cybersecurity needs requires high-level leadership, effective coordination, clearly mandated institutions, and functional governance mechanisms. Urgent action is needed to set up an interim governance model, underpinned by the National Cybersecurity Council (NCC), and the National Cybersecurity Coordinator. These institutions will prepare the ground for an optimal, permanent and centralized model of governance led by a competent national cyber authority (See Table 2).

Strategic Objective 1.1: Establish the model of national cybersecurity governance and supporting institutional and operational mechanisms.

Actions:

1.1.1 **Appoint a National Cybersecurity Coordinator**. Designate a high-level official responsible for coordinating all national cybersecurity efforts, ensuring alignment across various government agencies and sectors.

1.1.2 **Appoint Cybersecurity Focal Points**. Identify and appoint liaisons at each MAC participating in the NCC, and responsible for cybersecurity coordination on behalf of their governmental institutions.

1.1.3 **Establish the National Cybersecurity Council (NCC)**. Institute and empower the NCC co-chaired by the Ministry of State for Presidential Affairs (MoS) and the Ministry of Post and Telecommunications (MOPT). The main function of NCC is to define strategic directions and coordinate national cybersecurity efforts, working closely with the National Cybersecurity Coordinator.

1.1.4 **Establish the operational basis for NCC and the National Cybersecurity Coordinator.** Appoint a secretariat, providing organizational and administrative support to NCC and the National Coordinator. Appoint designated and seconded officials from the ministries, agencies and main stakeholders to support NCC, its committees and its Technical Task

Force as the initial incident response capability for cyber events of national significance. (Pillar 2 specifies the incident response role of this Task Force).

1.1.5 Develop a Strategic Roadmap for National Cybersecurity Governance. Develop and adopt a Roadmap Document specifying the short-term and long-term plans for transitioning from an interim model to a permanent governance model. The long-term model will involve creating a national competent authority for cybersecurity - the National Cybersecurity Agency (NCA), and transitioning the NCC and the National Cybersecurity Coordinator to advisory roles.

Table 2. Two-Phase Model of National Cybersecurity Governance

Key Mandates	Short-Term (2024-2026)	Long-Term (2027 onwards)
National Coordination	● NCC ● National Cybersecurity Coordinator	● NCC (advisory) ● National Cybersecurity Advisor ● National Cybersecurity Agency (NCA) and the Director of NCA
Operational Aspects	● NCC Technical Task Force	● Incident Response Unit/Department under the NCA
Strategy, Policy and Legislative Development	● MOPT ● NCC Strategy, Policy and Legislative Committee	● NCC Strategy, Policy and Legislative Committee ● MOPT and line ministries and agencies ● NCA's policy unit/department
Regulatory Functions	● NCC Regulatory Committee ● Sectoral regulators (LTA, CBL, LEC)	● NCC Regulatory Committee ● Sectoral regulators (LTA, CBL, LEC)
Supervision and Oversight	● Sectoral regulators (LTA, CBL, LEC)	● NCC Supervision and Oversight Unit/Department ● Sectoral regulators (LTA, CBL, LEC)

1.2 Enabling Policy, Legal and Regulatory Environment

Liberia must urgently adopt a unified policy and regulatory framework to address cybersecurity gaps in existing policies, legislation, and regulations. Reforms are needed within the telecommunications regulatory framework and other sectoral regulations, including those for the financial and electricity sectors.

Strategic Objective 1.2: Establish the fundamental policy, legal and regulatory frameworks to support national cybersecurity implementation.

Actions:

1.2.1 Develop and Adopt the Primary Law on Cybersecurity (National Cybersecurity Act). Create a legal framework that serves as the fundamental act for cybersecurity governance in Liberia. This law is essential to ground the NCS. It will define the roles, responsibilities, and mandates of key institutions, outline measures for managing cyber risks, protect networks and digital infrastructure, and establish cybersecurity compliance and reporting obligations for essential service providers.

1.2.2 Institute Supporting Legislative Frameworks. Using the National Cybersecurity Act as a basis, develop primary legislation to address:

- **Cybercrime Act.** Review and adopt the cybercrime-specific provisions of the Draft Cybercrime Act 2021.
- **Data Protection and Privacy Act.** Review and adopt the draft legislation on data protection and privacy, ensuring the cybersecurity provisions are aligned with the NCS.
- **Critical Infrastructure Act or Regulation**. Specify cybersecurity requirements for designated critical infrastructure sectors and entities in Liberia, providing procedural detail to support the National Cybersecurity Act.

1.2.3 Ensure the Alignment of the Law with Related Legislation. Conduct legal and regulatory analysis to identify to identify gaps, relationships, and synergies with the NCS, NCA and supporting frameworks, with focus on following key themes:

- National security.
- Digital government.
- Telecommunications.
- Emerging technologies.
- Innovation and intellectual property.
- Consumer protection.

- Child protection.
- Digital trade and e-commerce, e-signatures, e-transactions.

1.2.4 Draft Sector-specific Cybersecurity Regulations. Develop and enact sector-specific cybersecurity requirements that will be enforced through existing regulators and operating licences stipulating minimum cybersecurity standards, certification, audit, supervision, and oversight procedures for priority sectors, including:

- Telecommunications
- Banking and finance
- Energy
- Transportation (maritime, aviation, railway, municipal)
- Public sector (governmental institutions)
- Healthcare

1.2.5 Adopt Standard Operating Procedures. Create instructions, standard operating procedures, and guidance to operationalize the cybersecurity mandate by leading institutions. This package should include, but is not limited to:

- Incident response, information exchange, threat intelligence, reporting, disclosures and public communication.
- Public private partnerships in cybersecurity
- Cybersecurity service procurement, and outsourcing of services
- Minimum acceptable cybersecurity standards

Strategic Pillar 2. Protect.

The increasing frequency and scale of incidents affecting Liberia's infrastructure calls for a coordinated plan to secure national cyberspace. This plan should be based on a combination of institutional, regulatory, and procedural approaches, leveraging existing IT investments and integrating emerging enterprise-level cybersecurity capacities within governmental institutions and critical infrastructure (CI) entities in Liberia.

2.1 Establish National Incident Response Capacity

Liberia needs to create institutional capability to prepare for, prevent and respond to incidents of national significance. Given the emerging nature of national cybersecurity governance, planning for these capabilities should differentiate between immediately applicable steps based on current resources and longer-term aspirations (See Table 3).

Strategic Objective 2.1: Establish the national incident response capability for cyber resilience and incident response coordination.

Actions:

2.1.1 Establish the Incident Response Task Force under the National Cybersecurity Council. Set up an interagency task force to provide incident response planning and coordination at operational and technical levels, consisting of IT security team leaders in governmental institutions and critical infrastructure entities. The Task Force should report to the National Cybersecurity Coordinator and assigned leads by function.

2.1.2 Plan for National Large-Scale Incidents. Develop and validate a national incident response plan outlining key steps and procedures for cyber crisis management, including response coordination, cyber liaisons, interagency communication, assessment, classification and categorization of incidents, declaration of incidents, and national cyber emergency.

2.1.3 Conduct National Cyber Exercise and Cyber Drill. Conduct a national table-top exercise and cyber drill to support incident response coordination. The activity will serve as a diagnostic instrument, identifying the existing gaps in readiness, response and recovery.

2.1.4 Incident Reporting. Develop a procedure for mandatory and voluntary reporting of cyber incidents by the governmental institutions, business, academic to the office of the National Cybersecurity Coordinator, Technical Task Force and sectoral regulators.

2.1.5 Develop a Roadmap for the National Incident Response Unit. As part of the planning for the National Cybersecurity Agency, develop a roadmap for establishing a national incident response unit, such as a Computer Security Incident Response Team (CSIRT) or Security Operations Center (SOC).

Table 3. Phased Approach to Strategic Objective 2.1

Actions	Short-Term (2024-2026)	Long-Term (2027 onwards)
2.1.1 Establish the Incident Response Task Force under the NCC	Establish the Incident Response Task Force; define pathway for membership in the Forum of Incident Response and Security Teams (FIRST)	Fully operational national CSIRT as a Incident Response Coordination Unit under the NCA, and member of FIRST.
2.1.2 Plan for National Large-Scale Incidents	Develop a Plan for National Large-Scale Incidents	Update the Plan for National Large-Scale Incidents
2.1.3 Conduct National Cyber Exercise and Cyber Drill	Conduct initial National Cyber Exercise and Cyber Drill (under the NCC)	Conduct annual National Cyber Exercise and Cyber Drill (under the NCA)
2.1.4 Incident Reporting	Establish procedure for mandatory and voluntary reporting of cyber incidents (under NCC)	Refine procedure for mandatory and voluntary reporting of cyber incidents (under the NCA)
2.1.5 Develop a Roadmap for the National Incident Response Unit	Develop the Roadmap for the National Incident Response Unit	Implement the Roadmap for the National Incident Response Unit or CSIRT

2.2 Strengthen National Cyber Readiness

Liberia's cybersecurity investments should be guided by a systematic approach to managing and mitigating cyber risks. This requires introducing a unified framework specifying a common risk management approach and baseline measures establishing a minimally acceptable level of cybersecurity at designated institutions and entities.

Strategic Objective 2.2: Establish the national framework for cyber resilience and incident response.

Actions:

2.2.1 **Prepare a National Cybersecurity Framework.** Articulate a clear framework for managing cyber risks at the national level, consisting of structured procedures, instructions, and protocols providing technical directives for a shared risk management approach.

- Define processes and requirements for conducting national and sector-specific risk assessments, as well as implementing risk monitoring, analysis, and reporting mechanisms.
- The requirements should include provisions for a register of risks and integration of an analysis of threat landscape, common vulnerabilities. The assessments should provide recommended mitigation measures, based on centralized review of cybersecurity incidents.

2.2.2 **Baseline Cybersecurity Measures.** Define the fundamental practices, rules and requirements to establish a minimum level of cybersecurity at public sector and critical infrastructure entities.

- Apply the NIST Framework Functions (Identify, Protect, Detect, Respond, Recover) as overarching guidance.
- Adapt these measures to sectoral regulations and cybersecurity essentials for small and medium businesses, universities, civil society, and other non-state organizations.
- Specify requirements for applying secure-by-design principles to new IT and digital infrastructure investments.

Table 4. Phased Approach to Strategic Objective 2.2

Objectives	**Short-Term (2024-2026)**	**Long-Term (2027 onwards)**
2.2.1 Institute a National Cybersecurity Framework	Develop and Institute the National Cybersecurity Framework	Update the National Cybersecurity Framework
2.2.2 Institute Baseline Cybersecurity Measures	Develop and Institute the Baseline Cybersecurity Measures	Update the Baseline Cybersecurity Measures

2.3 Strengthen Operational Capacity to Combat Cyber Crime

Liberia is committed to overhauling the legal and regulatory basis for cybercrime prevention by developing comprehensive legislation on cybercrime. This framework will require operational measures to support the implementation and enforcement of key provisions.

Strategic Objective 2.3: Facilitate the Adoption and Enforcement of Cybercrime Legislation

Actions:

2.3.1 **Accelerate the Adoption of Comprehensive Cybercrime Framework.** Review and update the Draft Cybercrime Act, focusing on cybercrime issues (penal and procedural frameworks, enforcement, jurisdiction, and international cooperation). Protection of critical infrastructure should be decoupled from the National Cybersecurity Act, and addressed in the Critical Infrastructure Act.

2.3.2 **Institute a Cybercrime Reporting Channel at the Liberian National Police.** Set up an online portal for reporting cybercrimes, accessible to citizens and businesses. This channel should be integrated with the national incident reporting portal.

2.3.3 **Improve Technical Infrastructure and Capabilities to Combat Cybercrime.** Allocate resources to improve and upgrade the equipment, networks, and infrastructure needed to conduct cybercrime investigations at the national authorities mandated to investigate and prosecute cybercrime (Liberian National Police, National Security Agency).

2.3.4 **Implement National Cybercrime Management System.** Facilitate the implementation of a cybercrime management system, integrated into the national criminal investigations system.

2.3.5 **Develop Technical and Operational Capacity for Cybercrime.** Conduct regular capacity-building training for state personnel with cybercrime-related functions, including civilian agencies, police, security forces, other law enforcement agencies, judiciary, and prosecutors. Training topics should include fundamentals of cybercrime legislation, research, prevention, response, investigation, digital forensics, and cyber threat intelligence.

Table 5. Phased Approach to Strategic Objective 2.2

Objectives	Short-Term (2024-2026)	Long-Term (2027 onwards)
2.3.1 Accelerate the Adoption of a Comprehensive Cybercrime Framework	Adopt the Comprehensive Cybercrime Framework	Enforce and implement the Comprehensive Cybercrime Framework
2.3.2 Institute Cybercrime Reporting Channel at the Liberian National Police	Set up the Cybercrime Reporting Channel	Evaluate possible merger with the NCA's channels
2.3.3 Improve Technical Infrastructure for Cybercrime	Improve and upgrade technical investigative infrastructure	Evaluate the need for additional investments in technical infrastructure
2.3.4 Implement National Cybercrime Management System	Draft the concept of operations for the National Cybercrime Management System	Implement the National Cybercrime Management System
2.3.5 Develop Technical and Operational Capacity for Cybercrime	Implement initial activities for technical and operational capacity	Continue strengthening technical and operational capacity

Strategic Pillar 3. Sustain.

The long-term sustainability of cybersecurity and the governance mechanisms proposed in this strategy depend on developing a market for cybersecurity skills and capabilities supported by local expertise, a skilled workforce, and a cyber-aware society. Regulations must ensure that both the private and public sectors utilize these local skills. Achieving this requires fostering a "whole-of-society" culture of cybersecurity and creating an ecosystem that supports cybersecurity education, training, and certification. Additionally, it involves adopting best practices and actively participating in global and regional cybersecurity cooperation and diplomacy. Finally, regulatory measures should require operators of digital and cyber infrastructure to maintain cybersecurity teams and capabilities within Liberia as a condition of their license to operate.

3.1 Improve National Cybersecurity Education

Liberia's education system is responding to market demands for a skilled cybersecurity workforce. These initiatives hold the promise of improving cyber resilience, innovation and public awareness. However, additional support is needed to ensure the sustainable development of a cybersecurity workforce and the supply of job-ready graduates with required expertise to address requirements and real-time needs to secure Liberia's cyberspace.

Strategic Objective 3.1: Establish and strengthen the foundations of cybersecurity education.

Actions:

3.1.1 **Define the National Cybersecurity Education Framework.** Develop a general framework for cybersecurity education, aligned with international standards, specifying the criteria and requirements applicable to the formal education system (primary, secondary, tertiary) and professional training, Technical and Vocational Education and Training (TVET) institutions, including programs for upskilling and re-skilling of workforce.

3.1.2 **Mainstream Digital Safety and Digital literacy in the Educational Curricula.** Adopt, adapt and mandate Digital Safety and Digital Literacy frameworks such as the DigComp 2.0 into the curriculum of formal education and TVET programs.

3.1.3 **Designate a Cybersecurity Education Cluster.** Identify universities and TVET institutions that provide cybersecurity training, certification, and degree programs, and endorse them as certified providers of the cybersecurity curriculum in Liberia. Ensure that professional training, qualification, upskilling and re-skilling programs commissioned by

governmental institutions and state-owned enterprises are competitively awarded to local providers.

3.1.4 Support National Cybersecurity Research and Learning. Promote thought leadership, collaboration, partnerships, and information exchange among the cybersecurity education cluster, including the development of cybersecurity projects by Liberia's National Research and Academic Network. Facilitate cybersecurity research initiatives with practical applications at governmental institutions.

3.1.5 Strengthen the Relationships between Cybersecurity Education and Employer Organizations. Promote linkages between cybersecurity training institutions and employers seeking a skilled cyber workforce through incentive programs including tax credits for employers who hire interns and graduates from the local cyber talent pool.

3.1.6 Facilitate cybersecurity education initiatives to increase the representation of women in cybersecurity professions. Promote initiatives aimed at attracting and retaining girls and women in cybersecurity career tracks.

Table 6. Phased Approach to Strategic Objective 3.1

Objectives	Short-Term (2024-2026)	Long-Term (2027 onwards)
3.1.1 Define the Cybersecurity Education Framework	Define the Cybersecurity Education Framework jointly with the Ministry of Education and other GoL stakeholders	Implement and enforce the Cybersecurity Education Framework
3.1.2 Develop and integrate cybersecurity components in the curricula	Develop and integrate cybersecurity components in the formal education and TVET curricula	Implement the delivery of cybersecurity components in the formal education and TVET curricula
3.1.3 Identify and designate the cybersecurity education cluster	Identify and designate the cybersecurity education cluster	Refine and support the cybersecurity education cluster
3.1.4 Support National Cybersecurity Research and Learning	Conduct preparatory activities to support research and learning	Implement activities to support research and learning

3.1.5 Strengthen the Relationships between Cybersecurity Education and Employer Organizations	Strengthen relationships through recurrent activities	Continued as a recurrent activity
3.1.6 Facilitate Cybersecurity Education Initiatives Supporting Women	Promote initiatives supporting women in cybersecurity	Continued as a recurrent activity

3.2 Promote National Cybersecurity Awareness

Promoting awareness and knowledge of digital safety among the general population is a critical component of national cybersecurity strategy. An informed and cyber-aware society can significantly reduce the prevalence of cybercrime and mitigate associated risks on a national scale. By educating citizens about digital hygiene practices, recognizing and responding to cyber threats, and understanding the importance of safeguarding personal information, Liberia can build a resilient and secure digital ecosystem. Comprehensive awareness campaigns, targeted educational initiatives, and continuous community engagement are essential to build a culture of cybersecurity, ultimately strengthening national security and enhancing the overall digital well-being and resilience of Liberian society.

Strategic Objective 3.2: Support Cybersecurity Awareness and Cybersecurity Culture.

Actions:

3.2.1 Conduct National Cybersecurity Awareness Campaigns. Designate October as National Cyber and Digital Awareness Month. Implement comprehensive information and awareness-building campaigns targeting citizens and society throughout Liberia. These campaigns will be conducted under the auspices of the National Cybersecurity Council to ensure a coordinated and effective approach. The aim is to educate the public on the importance of cybersecurity and provide practical advice on how to protect personal and organizational data.

Use various media channels, including social media, television, radio, and print, to reach a broad audience. These campaigns will emphasize the importance of cybersecurity in everyday life and provide practical tips for staying safe online. The campaigns will be

designed to resonate with different segments of the population, ensuring widespread engagement and impact.

3.2.2 Facilitate Cybersecurity Awareness Activities. Promote cross-sectoral and interagency collaboration to support cybersecurity awareness objectives. This includes encouraging partnerships and joint activities that engage civil society organizations, media outlets, academic institutions, and corporate entities. By leveraging the strengths and resources of these diverse stakeholders, the aim is to create a comprehensive and unified approach to cybersecurity awareness.

3.2.3 Prepare and Publish Awareness Raising Materials. Establish an online portal under the National Cybersecurity Coordinator to serve as a central hub for cybersecurity awareness and capacity-building materials. This portal will provide easy access to educational resources, guidelines, and best practices, helping citizens and organizations stay informed and prepared against cyber threats. The portal will be regularly updated to reflect the latest cybersecurity developments and recommendations.

Table 6. Phased Approach to Strategic Objective 3.2

Objectives	Short-Term (2024-2026)	Long-Term (2027 onwards)
3.2.1 Conduct National Cybersecurity Awareness Campaigns	Adopt October as Digital Safety and Cybersecurity Month Implement Cybersecurity Awareness Campaigns Implement Media Campaigns to Reach a Broad Audience	Continue Campaigns with Updated Content and Wider Reach Continue Campaigns with Updated Content and Wider Reach
3.2.2 Facilitate Cybersecurity Awareness Activities	Promote Cross-Sectoral, Interagency Collaboration and Partnerships	Sustain and Expand Collaborative Efforts
3.2.3 Launch a Dedicated Cybersecurity Awareness Portal	Establish and Promote the Online Portal for Public Access	Maintain And Enhance the Portal with New Content and Features

3.3 Advance International Cooperation

National cybersecurity stakeholders in Liberia stand to gain multiple benefits from pursuing international cooperation in the field of cybersecurity. Engaging with global and regional partners allows Liberia to benefit from shared knowledge, resources, and best practices. Such engagement must be strategic, centrally coordinated, and aligned with national cybersecurity objectives.

Strategic Objective 3.3: Strengthen Liberia's Participation in Global Cybersecurity Cooperation Frameworks.

Actions:

3.3.1 Ensure Strategic Alignment of National Cybersecurity Frameworks with Regional and Global Frameworks. Align Liberia's national cybersecurity policies and frameworks with regional and global standards. This includes adopting the common cybersecurity approaches promoted by the Economic Community of West African States (ECOWAS) and the African Union. Regular reviews and updates, rooted in analyses of global cybersecurity trends will ensure continued alignment with international best practices.

3.3.2 Accede to International Cybersecurity and Cybercrime Conventions and Related Initiatives. Join international conventions and initiatives, such as the Budapest Convention on Cybercrime and the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention). Participation in these frameworks will enable Liberia to collaborate effectively on global cybersecurity issues, benefiting from international expertise and support.

3.3.3 Membership in the Forum of Incident Response and Security Teams (FIRST). Membership in FIRST is a key step to improve Liberia's cybersecurity capabilities. Integrating into this global incident response network will enhance Liberia's ability to manage cybersecurity incidents by providing access to shared knowledge and tools for developing a national incident response framework. Participation in FIRST will also promote collaboration with international experts, helping Liberia tackle emerging cyber threats and contributing to broader cybersecurity resilience.

3.3.4 Participate in Global Cybersecurity Initiatives. Actively engage in globally recognized cybersecurity initiatives and cyber norms frameworks, such as the International Ransomware Initiative. This participation will enhance Liberia's capabilities in addressing cyber threats and contribute to the development of international cybersecurity policies. Initiate a public communication and advocacy campaign, alongside hosting strategic meetings, to re-engage Liberia with regional and international partnerships and

cooperation platforms. This effort will reposition Liberia as an active participant in global cybersecurity discussions and collaborations.

3.3.5 Appoint Cybersecurity Ambassador and Expand Public Communication and International Engagement. Identify and appoint within the diplomatic cadre a Cybersecurity Ambassador for Liberia, as a position responsible for advancing the international cybersecurity partnerships. Under the leadership of this position, and in coordination with the national cybersecurity bodies, initiate a public communication and advocacy campaign to highlight Liberia's commitment to cybersecurity and re-engage with regional and international partnerships. Hosting strategic meetings and participating in international forums will position Liberia as an active participant in global cybersecurity discussions and collaborations.

3.3.6 Establish Bilateral and Multilateral Partnerships. Develop and strengthen bilateral and multilateral partnerships with other nations and international organizations. These partnerships will facilitate the exchange of information, expertise, and resources, enhancing Liberia's cybersecurity capacity and resilience.

3.3.7 Leverage International Support for Capacity Building. Seek technical assistance, training programs, and financial support from international partners to build local cybersecurity capabilities. This includes developing training programs for cybersecurity professionals, enhancing incident response capabilities, and supporting public awareness initiatives.

Table 7. Phased Approach to Strategic Objective 3.3

Objectives	Short-Term (2024-2026)	Long-Term (2027 onwards)
3.3.1 Ensure Strategic Alignment with Regional and Global Frameworks	Align national policies with ECOWAS and African Union standards	Conduct regular reviews to ensure ongoing alignment
Conduct preparatory activities to join international conventions	Conduct preparatory activities to join international conventions	Officially join and actively participate in international conventions
3.3.3 Participate in Global Cybersecurity Initiatives	Engage in global cybersecurity initiatives and forums	Sustain and expand participation in international cybersecurity initiatives
3.3.4 Appoint Cybersecurity Ambassador and Expand	Appoint Cybersecurity Ambassador. Launch	Maintain and enhance international engagement

Public Communication and International Engagement	communication campaigns and host strategic meetings	efforts
3.3.5 Establish Bilateral and Multilateral Partnerships	Develop partnerships with other nations and international organizations	Strengthen and expand bilateral and multilateral collaborations
3.3.6 Leverage International Support for Capacity Building	Seek technical assistance and training programs	Sustain and enhance capacity-building initiatives with international support

3.4 Leverage Regulatory Authority to Create a National Market for Cybersecurity Skills

Creating a national market for cybersecurity skills in Liberia requires leveraging the authority of regulators across critical infrastructure sectors. This approach ensures that the necessary cybersecurity capabilities are embedded within the operations of all critical infrastructure providers, significantly improving national resilience and creating a demand for local expertise.

Strategic Objective 3.4: Use Regulatory Authority to Mandate Resident Cybersecurity Teams and Capabilities.

Regulators in sectors such as banking, energy, and telecommunications must require licensed operators to maintain dedicated cybersecurity teams and capabilities within the country. These Liberia-based teams will be responsible for monitoring, incident response, and ensuring ongoing cybersecurity readiness. Embedding this requirement into the licensing conditions for operating in Liberia will ensure that critical infrastructure operators develop and sustain local cybersecurity expertise that creates demand for these skills in the national economy.

Actions:

3.4.1 **Regulatory Mandates for Cybersecurity Teams and Capabilities.** Develop regulations that mandate the establishment and maintenance of cybersecurity teams and capabilities by critical infrastructure operators, including banks, energy providers, and telecommunications companies. These teams must be based in Liberia and capable of monitoring, incident response, and maintaining cybersecurity protocols.

3.4.2 **Incorporate Cybersecurity Requirements into Licensing.** Embed the requirement for maintaining a local cybersecurity team into the licensing conditions for operating critical infrastructure services in Liberia. Ensure that these requirements are clear, enforceable, and regularly audited. Requirements must include schedules that establish a compulsory timeframe and criteria for reporting on major cyber events that impact critical infrastructure and their end users.

3.4.3 **Monitoring and Compliance.** Establish appropriate monitoring and compliance mechanisms to ensure that critical infrastructure operators adhere to the mandated cybersecurity requirements. This includes regular audits, reporting obligations, and penalties for non-compliance.

3.4.4 **Collaboration with Industry Stakeholders.** Promote collaboration between regulatory authorities, industry stakeholders, and cybersecurity education providers to ensure a steady supply of skilled cybersecurity professionals. Promote public-private partnerships to enhance the overall cybersecurity ecosystem in Liberia.

Table 8. Phased Approach to Strategic Objective 3.4

Objectives	**Short-Term (2024-2026)**	**Long-Term (2027 onwards)**
3.4.1 Develop Regulatory Mandates	Create regulations for mandatory cybersecurity teams	Review and update regulations as needed
3.4.2 Incorporate Cybersecurity into Licensing	Embed requirements into licensing conditions	Ensure ongoing compliance and enforce penalties
3.4.3 Establish Monitoring and Compliance Mechanisms	Set up monitoring and compliance frameworks	Conduct regular audits and enforce compliance
3.4.4 Promote Collaboration with Stakeholders	White paper on public-private partnerships (PPP) Initiate public-private partnerships	Sustain and expand PPP efforts

Success Factors

The successful implementation of the NCS and its Action Plan relies on an effective governance model, adequate resources, and a robust monitoring and evaluation framework.

Effective Implementation of Actions and Activities

The success of Liberia's inaugural NCS is dependent on effective implementation of the actions and activities, leading to achievement of the stated objectives. Given the significant investment in digital development and the increasing dependency on ICT infrastructure, time is of the essence. Addressing governance and structural issues simultaneously is essential, and leveraging regulatory authority to incentivize private sector participation will be critical for the NCS's success.

The strategy's implementation demands a robust governance structure with high-level support, clear roles, and responsibilities tied to specific performance targets within a defined timeframe. The Action Plan accompanying this strategy outlines indicative responsibilities among Government of Liberia (GoL) institutions and provides a timeline for NCS activities. Each action in the Action Plan must be assessed against performance targets, which can be indicators or outputs to validate successful implementation.s.

The Action Plan distinguishes between one-time activities, such as establishing procedures and periodic reviews, and recurrent activities, such as awareness campaigns and partner engagement. It clearly identifies responsible institutions and actors with primary and secondary roles, facilitating coordination and division of responsibilities. The primary institution is accountable for implementation, but it will need support from secondary role actors.

The implementation of the NCS is structured in two phases:

1. **Phase One (2024-2026)**: This phase focuses on addressing immediate and short-term needs. The success of the NCS objectives will hinge on establishing three main national-level institutions: the National Cybersecurity Council, the National Cybersecurity Coordinator, and the Technical Task Force, which serves as the precursor to the incident response capability. These institutions can be set up with minimal resources by utilizing existing mandates and positions, providing the necessary governance structure to operationalize the NCS. The roles of the Council, Coordinator, and Task Force can be integrated within the existing CIO (Chief Information Officer) mechanisms and the Chief CIO role in GoL institutions.

2. **Phase Two (2027-2029)**: This phase prepares for medium and long-term arrangements. It is crucial to lay the groundwork for establishing a national competent authority for

cybersecurity, the National Cybersecurity Agency (NCA), and transitioning the National Cybersecurity Council and Coordinator to advisory roles.

In both phases, strong support from sectoral institutions is essential. Each sector and critical infrastructure entities should adopt the main principles of the NCS to drive sector-specific, customized planning and actions.

Resource Allocation and Sustainable Funding

Sustaining the government's efforts in cybersecurity, digital security, and development will continuously be a resource challenge. Activating the private sector is vital. Government resources and budgets must be effectively supplemented through creative public-private partnerships and the use of regulation to create a natural market for IT. This approach will also transfer some responsibility for national cybersecurity to operators of critical infrastructure, particularly in telecommunications and energy.

The NCS will require a commitment of resources drawn from both domestic and development partner sources. Domestic sources include the existing IT and IT security budgets of GoL institutions. Development partner sources encompass existing and planned technical assistance, budgetary contributions, and project-specific resource mobilization opportunities.

Government revenues are not sufficient to cover all the costs required for the implementation of the NCS Action Plan. Current budgets and expenditures are adequate for staffing, minimal technical infrastructure, initial capacity building, and administrative and operational expenses. However, the budgets of GoL institutions with assigned actions under the Action Plan should be revisited upon the adoption of the NCS. This budgeting exercise must prioritize creating Liberia's national incident response capacity.

From a broader national perspective, the NCS will require additional resource commitments to support compliance, such as infrastructure upgrades, personnel costs, and procurement of services. While the resource requirements of the NCS can be significant, these investments are essential to safeguard the digital future of Liberia.

Liberia will need to harness public-private partnerships and utilize regulatory measures to foster a market for IT services. This approach will not only address immediate cybersecurity needs but also ensure the long-term sustainability and resilience of its digital infrastructure.

Monitoring and Evaluation

Monitoring and evaluation (M&E) is critical to the successful implementation of the NCS. The strategy will need to be reviewed annually, and adjustments will need to be made as technology, policy, and the needs of the country evolve. It should be seen as a living document, with ongoing monitoring and evaluation to ensure its effectiveness for Liberia's benefit.

The established M&E system and best practices as part of national strategic planning and implementation in Liberia will guide the monitoring and evaluation of the NCS. A comprehensive review of the NCS implementation is scheduled after the first three years (indicative year: 2027), with a final review in year five (indicative year: 2029). The National Cybersecurity Council, with support from the Ministry of Post and Telecommunications (MOPT), will conduct these reviews.

Additionally, the MOPT will conduct annual surveys among responsible governmental institutions to collect implementation status updates, feedback on the NCS, and insights into encountered challenges and opportunities. This continuous feedback loop will ensure the NCS remains relevant and responsive to changing circumstances.

.

Annex A. Action Plan

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
Strategic Pillar 1. Build.					
Strategic Objective 1.1: Establish the model of national cybersecurity governance and supporting institutional and operational mechanisms.					
1.1.1 Appoint a National Cybersecurity Coordinator.	Office of the President (Ministry of State for Presidential Affairs)	Ministry of Posts and Telecommunications (MOPT)	Established and mandated position	Q4 2024	
1.1.2 Appoint Cybersecurity Focal Points.	Various Government of Liberia (GoL) institutions	National Cybersecurity Council (NCC)	Established and mandated positions	Q4 2024	
1.1.3 Establish the NCC.	Ministry of State for Presidential Affairs	MOPT	Established and mandated institution	Q4 2024	

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
1.1.4 Establish the operational basis for NCC and the National Cybersecurity Coordinator.	Ministry of State for Presidential Affairs	MOPT, other Ministries	Established and mandated operational roles	Q1 2025	
1.1.5 Develop a Strategic Roadmap for National Cybersecurity Governance.	MOPT	NCC	Adopted Roadmap	Q4 2025	
Strategic Objective 1.2: Establish the fundamental policy, legal and regulatory frameworks to support national cybersecurity implementation.					
1.2.1 Develop and Adopt the Primary Law on Cybersecurity (National Cybersecurity Act).	Legislature of Liberia, Ministry of Justice	MOPT	Adopted legislation	Q3 2025	
1.2.2 Institute Supporting Legislative Frameworks (i.e. Cybercrime Act, Data Protection and Privacy Act, and Critical Infrastructure Act or Regulation).	Legislature of Liberia, Ministry of Justice	Ministries of National Defense, Health, Education, Public Works, etc.	Adopted legislation	Q4 2025	
1.2.3 Ensure the Alignment of the Law with Related Legislation.	Ministry of Justice	MOPT, Liberia Telecommunications Authority (LTA), Central Bank of Liberia, etc.	Revised and approved legislation	Q4 2025	

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
1.2.4 Draft Sectoral Regulations on Cybersecurity (telecommunications, banking and finance, energy, transportation, public sector, healthcare).	MOPT, LTA, Central Bank of Liberia	Ministry of Transport, Ministry of Health, Ministry of Mines and Energy, etc.	Adopted regulations	Q4 2025	
1.2.5 Adopt an Operational Package.	NCC	MOPT, LTA	Adopted operational procedures	Q1 2026	
Strategic Pillar 2. Protect.					
Strategic Objective 2.1: Establish the national incident response capability for cyber resilience and incident response coordination.					
2.1.1 Establish the Incident Response Task Force under the National Cybersecurity Council.	NCC	MOPT, National Security Agency	Established and mandated Task Force	Q4 2024	
2.1.2 Plan for National Large-Scale Incidents.	NCC	Ministry of National Defense	Adopted Plan	Q2 2025 (initial)	Q3 2027 (update)
2.1.3 Conduct National Cyber Exercise and Cyber Drill.	NCC	Ministry of National Defense,	Annual events	Q2 2025 (initial)	Recurrent annually

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
		National Security Agency		Recurrent annually thereafter	
2.1.4 Establish Procedures for Incident Reporting.	NCC	MOPT, LTA, Central Bank of Liberia, etc.	Adopted Procedures	Q2 2025	
2.1.5 Develop a Roadmap for the National Incident Response Unit.	NCC	MOPT	Adopted Roadmap	Q3 2025	
Strategic Objective 2.2 Establish the national framework for cyber resilience and incident response.					
2.2.1 Prepare a National Cybersecurity Framework.	NCC, MOPT	Ministry of Justice	Adopted Framework	Q3 2025	Q3 2027 (update)
2.2.2 Baseline Cybersecurity Measures.	NCC, MOPT	Ministry of Justice	Adopted Measures	Q4 2025	Q3 2027 (update)
Strategic Objective 2.3 Facilitate the Adoption and Enforcement of Cybercrime Legislation Actions.					
2.3.1 Accelerate the Adoption of Comprehensive Cybercrime Framework.	Ministry of Justice	Legislature of Liberia, MOPT	Adopted Cybercrime Framework	Q3 2025	Q3 2027 (update)

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
2.3.2 Institute a Cybercrime Reporting Channel at the Liberian National Police.	Ministry of Justice, Liberia National Police	MOPT, NCC	Functional Reporting Channel	Q1 2025	Q3 2027 (refine)
2.3.3 Improve Technical Infrastructure and Capabilities to Combat Cybercrime.	Ministry of Justice, Liberia National Police	MOPT, NCC	Verified annual assessments of improved infrastructure and capabilities	Q3 2025 Recurrent annually thereafter	Recurrent annually
2.3.4 Implement National Cybercrime Management System.	Ministry of Justice, Liberia National Police	MOPT, NCC	Implemented National Cybercrime Management System	Q2 2025	
2.3.5 Develop Technical and Operational Capacity for Cybercrime.	Ministry of Justice, Liberia National Police	MOPT, NCC	Verified annual assessments of improved technical and operational capacity	Q3 2025	Recurrent annually
Strategic Pillar 3. Sustain.					

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
Strategic Objective 3.1: Establish and strengthen the foundations of cybersecurity education.					
3.1.1 Define the National Cybersecurity Education Framework.	Ministry of Education, NCC	Ministry of Gender and Social Protection, Universities	Adopted Framework document	Q4 2025	
3.1.2 Mainstream Digital Safety and Cyber literacy in the Educational Curricula.	Ministry of Education, NCC	Ministry of Gender and Social Protection, Universities	Adopted mainstreamed components	Q2 2026	Recurrent annually
3.1.3 Designate a Cybersecurity Education Cluster.	Ministry of Education, NCC	Universities	Approved document designating the Cluster	Q2 2026	Q4 2028 (revise)
3.1.4 Support National Cybersecurity Research and Learning.	Liberia Research And Education Network (LREN)	Ministries	Research outputs	Q3 2026	
3.1.5 Strengthen the Relationships between Cybersecurity Education and Employer Organizations.	Ministry of Education, NCC	Liberia Chamber of Commerce, Private Sector	Annual events	Q4 2026	Recurrent annually

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
3.1.6 Facilitate cybersecurity education initiatives supporting women.	Ministry of Gender and Social Protection	Ministry of Education, Private Sector	Annual events and activities	Q4 2026	Recurrent annually
Strategic Objective 3.2: Support Cybersecurity awareness and Cybersecurity Culture.					
3.2.1 Conduct National Cybersecurity Awareness Campaigns.	NCC	Ministries, Civil Society, Academic Institutions, Private Sector, International Partners	At least one annual campaign	Q3 2025 Recurrent annually thereafter	Recurrent annually
3.2.2 Facilitate Cybersecurity Awareness Activities.	NCC	Ministries, Civil Society, Academic Institutions, Private Sector, International Partners	At least 10 annual activities	Q3 2025 Recurrent annually thereafter	Recurrent annually
3.2.3 Prepare and Publish Awareness Raising Materials.	Office of the National Cybersecurity Coordinator	MOPT, Ministry of Education	At least 5 annual publications and/or releases	Q4 2025 Recurrent annually thereafter	Recurrent annually
Strategic Objective 3.3: Strengthen Liberia's Participation in Global Cybersecurity Cooperation Frameworks.					

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
3.3.1 Ensure Strategic Alignment of National Cybersecurity Frameworks with Regional and Global Frameworks.	NCC, MOPT, Ministry of Justice	Ministry of Foreign Affairs	Review Report with analysis and recommendations	Q4 2025 Recurrent annually thereafter	Recurrent annually
3.3.2 Accede to International Cybersecurity and Cybercrime Conventions and Related Initiatives.	NCC, MOPT, Ministry of Justice	Ministry of Foreign Affairs	Ratified Conventions	Q4 2026	Q4 2028 (Update)
3.3.3 Prepare and apply for nCSIRT membership in FIRST	NCC Technical Task Force		Secured membership in FIRST		Q2 2027
3.3.4 Participate in Global Cybersecurity Initiatives.	NCC, MOPT	Ministry of Foreign Affairs, Office of the President	Review Report with analysis and recommendations	Q4 2025 Recurrent annually thereafter	Recurrent annually
3.3.5 Appoint a Cybersecurity Ambassador and Expand Public Communication and International Engagement.	NCC, Ministry of Foreign Affairs	Office of the President	Appointed and mandated position; Review Report with analysis and recommendations	Q2 2025 Recurrent annually thereafter	Recurrent annually

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
3.3.6 Establish Bilateral and Multilateral Partnerships.	NCC, Ministry of Foreign Affairs	Office of the President	Review Report with analysis and recommendations	Q4 2025 Recurrent annually thereafter	Recurrent annually
3.3.7 Leverage International Support for Capacity Building.	NCC, MOPT, Ministry of Foreign Affairs	Office of the President	Review Report with analysis and recommendations	Q2 2025 Recurrent annually thereafter	Recurrent annually
Strategic Objective 3.4: Use Regulatory Authority to Mandate Resident Cybersecurity Teams and Capabilities.					
3.4.1 Regulatory Mandates for Cybersecurity Teams and Capabilities.	NCC, MOPT, LTA	Ministry of Finance and Development Planning (MFDP)	Review Report with analysis and recommendations	Q3 2025	
3.4.2 Incorporate Cybersecurity Requirements into Licensing.	LTA, MOPT	MFDP, NCC	Adopted requirements	Q4 2025	Q4 2028 (Update)
3.4.3 Monitoring and Compliance.	LTA, MOPT	MFDP, NCC	Monitoring and compliance report(s)	Q4 2025 Recurrent annually thereafter	Recurrent annually

Strategic Objectives and Actions	Implementing Entity		Indicators/ Outputs	Timeline (End Dates)	
	Primary	Secondary		2024-2026	2027-2029
3.4.4 Collaboration with Industry Stakeholders.	LTA, MOPT	MFDP, NCC	Review Report with analysis and recommendations	Q4 2025 Recurrent annually thereafter	Recurrent annually