Draft Cybersecurity Strategy

of the

Republic of Liberia

Prepared by the Liberia Telecommunications Authority (LTA)
In collaboration with the Inter-Agency Cybersecurity Working Group and Other Stakeholders

The public is encouraged to send inputs and comments on this draft document from February 27, 2020 to April 15, 2020 to the following emails:

support@lta.gov.lr or to dzotawontitus@gmail.com

Document ID# **GoL/NCS/LTA/Draft 0003/2020**

Liberia National Cybersecurity Strategy

1.0 EXECUTIVE SUMMA`RY

Liberia has been a part of over 100 nations without a national cybersecurity strategy. The International Telecommunications Union (ITU) has encouraged countries in this category to develop their cyber strategy using its guidelines. Using the ITU guidelines to develop, establish and implement a national cybersecurity strategy is desirable and necessary because the guidelines are based on principles, values and standards that matter in securing a national digital space. Liberia has adopted the ITU cybersecurity guidelines, successfully reversed the narrative that it did not have a national cyber strategy and has now re-positioned itself to effectively safeguard and protect its ICT ecosystem.

A cybersecurity strategy is critical for the safety of the internet. Liberia values and cherishes the internet for a variety of purposes including value addition to services. While the internet has proven to be essential for efficiency gains and other developmental outcomes, there is yet another side to it. Criminals exploit the internet to cause havoc, commit theft and launch cyber-attacks that can cause disruption of services. Our nation can no longer remain idle in this space; it shall provide awareness and prepare itself to combat cyber criminals and the threats they pose.

The internet and ICTs have unintentionally provided Cyber criminals with the tools that are capable of undermining digital platforms and services. Liberia is putting in place its national cybersecurity strategy to curtail cyber vulnerabilities and take advantage of the efficiency of digital platforms that can enhance transformation across Government, Education, Commerce, Health and other services. A resilient national digital infrastructure is critical in supporting transformative services. National digital infrastructure can provide Information technology platforms that facilitate the seamless operation of online services and facilities. Liberia's presence in cyberspace is a function of its digital infrastructure, content and the extent to which its people are connected.

Vulnerability in the national cyber space is a threat to Liberia's digital infrastructure. Vulnerability may lead to disruption of online services and compromise national data and other forms of content. Such disruptions can be consequential as they can have negative implications on national economy and security. Taking steps to secure digital infrastructure and services is a critical imperative under this national cybersecurity strategy. Liberia has outlined some measures to protect its national infrastructure and services from cyberattacks including the following:

A. To provide a governance framework and structures with corresponding authority and responsibilities for agenda setting, mobilizing resources, among others, for all cybersecurity matters;
B. To establish appropriate legal and regulatory frameworks to guarantee order, protect the innocence and privacy of users and criminalize attacks in Liberia's cyberspace;
C. To protect the physical, virtual and other Information Communications and Technology (ICT) assets within Liberia's cyberspace through the development of an effective mechanism that addresses and responds to cyber threats irrespective of its origin;

D. To help prevent cyberattacks against critical national infrastructure and ensure the safety of information networks by building competency and capability of primary stakeholders;
E. To ensure the safety of all online consumers by promoting awareness of cyber risks and developing measures to mitigate cyber risks and attacks;
F. To minimize potential damage arising from cyberattacks and develop capabilities to minimize the effect of cyberattacks through a robust incident management regime;

These objectives can be achieved through defined actions. In this regard, seven (7) areas of focus and priorities have been identified in pursuit of those objectives:

1. **Governance** – the establishment of the body responsible for all cybersecurity matters as the coordinating authority on cybersecurity operations is critical. The National Council on Cybersecurity shall be established as the highest decision making body on cybersecurity in Liberia;
2. **Incident Management** – The establishment of a Computer Emergency Response Team (CERT) as a hub for incident reporting, incident management and incident response is a critical necessity. A National CERT shall therefore be established;
3. **Capacity Building** – Regulatory staff, Policy Makers, Judges, Security and Law Enforcement Officers all need specialized skills to enable them to effectively confront and deal with cybersecurity incidents. Capacity building on a broad range of cybersecurity skills for relevant institutions shall be conducted in preparation of Liberia's readiness to manage its digital space.
4. **Culture** – Liberia shall promote a culture-sensitive cyber environment for its people. It shall provide awareness using different approaches to enlighten its people about the dangers and risks of cybercrime. It shall also designate national opinion leaders and other such eminent persons to help raise awareness on cyber security issues throughout the society. Such persons shall be designated Cybersecurity Champions for the nation;
5. **Legislation** – the enactment of relevant cybercrime legislation to criminalize cyber offences, prosecute offenders and protect both consumers and critical national infrastructure cybercrime targets from cyber criminals;
6. **Collaboration** – the establishment of partnership across the public, private and civil society sectors with all relevant stakeholders and actors towards securing Liberia's digital space since cybercrime does not know border;
7. **International Co-operation** – Liberia shall avail itself in working with development partners, international organizations, sub-regional, regional, continental and global organizations in consolidating the fight against cybercrime and enhancing cybersecurity.

Creating a secure cybersecurity environment requires a roadmap and clear strategy. Liberia's Cybersecurity Strategy is a combination of activities, technological, legal and other programs that taken together, contributes to creating a secure cyber environment. Across each activity is the indispensable role of skill requirements. This is why Cybersecurity concerns are not a one person business and together Liberians and their counterparts can provide a safe and secure environment for our infrastructure and services for the good of society.

Monrovia, July 2019

2.0 Introduction

AN OVERVIEW OF NATIONAL CYBERSECURITY STRATEGY

2.1 Introduction:

Liberia National Cybersecurity Strategy (LNCS) is a strategic document that identifies critical measures and operational actions to support the promotion of a secure Liberian cyberspace. Driven by its national vision **"to achieve a secure and resilient cyber environment for the protection of Liberia's digital space**" it illustrates ways to protect critical information infrastructure (CII) and online services. It also supports a responsive and sensible cyber user community. Underpinning the strategy are short, medium and long term mitigation measures that support a safe and resilient cybersecurity environment. These mitigation measures include the creation of an enabling legal and policy framework, ratifying all international agreements on cybersecurity, identifying operational goals and working with all partners in consolidating the fight against cybercrime.

Essentially, Liberia's Cybersecurity Strategy presents steps, programs and initiatives that it shall undertake to protect its national cyber-infrastructure, increase its security and consolidate its resilience. The strategy shall align its cybersecurity programs with other ICT-related objectives and priorities. It is not a stand-alone initiative as it seeks to integrate human capacity, infrastructure safety and online services, among others, in a mutually inclusive way. Identifying and closing potential cyber vulnerabilities will prevent material damage to the integrity of our nation and reduce the possibility of attacks that could disrupt services that ride on critical information infrastructure.

2.2 National Cybersecurity Vision:

The strategy sets out a clear purpose and outcome of what Liberia intends to achieve under its cybersecurity program. This value which guides its direction is articulated in its cybersecurity vision, **"to achieve a secure and resilient cyber environment for the protection of Liberia's digital space"**. Fulfilling this vision will enable Liberia to contribute to the overall vison of the African Union which seeks to create a secure digital space for Africa.

2.3 Cyberspace

Cyberspace is an interdependent network of critical and non-critical national information infrastructures. It is made up of a convergence of interconnected information and communication resources through the use of information and communication technologies (ICT). Generally, it encompasses all forms of digital engagements and transactional activities.

2.4 Liberia Cyberspace

Liberia's cyberspace refers to the interdependent network of critical national information infrastructure such as the terrestrial fiber cable, the internet exchange point, the infrastructure of the mobile network operator, data center and the database of institutions. Its cyberspace equally includes non-critical national information infrastructure such as a mask, a V-sat, a television and a radio station.

While disruption to non-critical infrastructure can have some impact, the real impact can be experienced across the nation when these infrastructure classified as critical national infrastructure, suffer vulnerability.

Vulnerabilities exist within cyberspace that can be used to exploit national economic interests and constitute threats to National Security. Liberia must prepare itself to tackle or address potential weakness as a result of its digital vulnerability. A first step can be a national assessment of cybersecurity vulnerabilities. Preparation could include ways to provide countermeasures in partnership with other legitimate state and non-state actors against cyber threat. Liberia has formulated its National Cybersecurity Strategy as one of the measures to demonstrate its readiness to deal with cyber threats.

3.0 What is Cyber Security?

Liberia subscribes to the Cybersecurity definition provided by the International Telecommunications Union (ITU). The Telecommunication Standardization Sector (ITU-T) Bureau of the ITU in its Recommendation X.1205, defines cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. It further provides that organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity has a direct correlation with cyberspace. Cybersecurity therefore strives to prevent or address Cyber-attacks on a specified cyberspace.

3.1 Cyber Attacks

Cyberattacks is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an ICT asset. It may lead to identity theft, fraud, extortion, malware, pharming and phishing. Spamming, spoofing, spyware and release of Trojans and, furthermore, manipulation of hardware, denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks and breach of access can be the result of a cyberattack. In addition, password sniffing, system infiltration, website defacement, private and public web browser exploits, instant messaging and social media abuse, and intellectual property theft matter in the cyberspace. Effective cybersecurity strategy provides ways to safeguard critical infrastructure and enhance trust in related systems.

3.2 A Call to Action

A call to action is a motivation to act in order to address a problem. To prevent cybercrime and secure Liberia's digital space requires a series of actions. Liberia's call to action is a series of interdependent activities that when implemented, will make its cybersecurity strategy successful. This strategy therefore has identified policy and regulatory interventions that seeks to prevent, minimize or address cyber-attack in Liberia's digital space. By identifying, defining and implementing these plans and activities, Liberia shall achieve a safe and resilient cybersecurity environment. Once this call to action is effectively implemented, people who use Liberia's cyberspace shall trust and rely on the internet and its digital infrastructure. This development could lead to situating Liberia's IT infrastructure as the true enabler for innovations.

Such initiatives will reduce the potential threats in cyberspace and safeguard Liberian online consumers.

3.3 Policy interventions and Activities

The call to action perspective of Liberia's cybersecurity strategy is a part of initiatives and bold actions that will positively impact the cyber landscape. As strategic interventions, they outline key priorities that must be addressed in Liberia's readiness to adequately secure its cyber space.

Policy Interventions	**Activities**
Make Cybersecurity a Policy Priority of the nation	1.1 Issue an Executive Order to make cybersecurity issue a matter of national security concern 1.2 The Executive Order should establish a National Council on Cybersecurity; 1.3 Membership of the Council shall include key stakeholders 1.4 The Order shall designate Chair of the Council 1.5 The Order shall also establish an Inter-agency working committee on cybersecurity matters
1.0 Create an appropriate Governance framework for Cyber Security	1.1 Establish a National Council on Cybersecurity as the body to provide direction on cyber programs. The Council shall have the authority to act as a management entity to define and clarify roles, responsibilities, processes, decision rights, and the tasks required to ensure effective implementation of the Strategy; 1.2 Develop and implement common ICT security standards across Government; 1.3 Provide a mechanism for periodic review and assessment of national cybersecurity policies, Regulations and programs. 1.4 Designate an agency (NSA) to oversee the implementation of the Strategy and establish performance targets for various ministerial or governmental departments, institutions responsible for specific aspects of the Strategy and subsequent action plan. 1.5 Establish an inter-agency working group
2.0 A. Make Liberia a signatory to international Conventions on Cybersecurity	2.1 Ratify the Malabo Convention – take action to domesticate the framework to drive the protection of critical cyber/ICT infrastructure, personal data and to encourage free flow of information with the aim of developing a credible digital space in Africa.

	2.2 Ratify the Budapest Convention – take action to ensure that Liberia harmonizes its national laws, improves its investigative techniques, and becomes a cooperating member among nations in fighting cybercrime.
3.0 Require that key actors and players in the ICT sector create their own CERTs	Individual banks, Mobile Network Operators, Security Agencies, Academic institutions, among others should have CERT in place
3.0 Develop National Incident Management Capabilities	2.1 Establish a centralized Computer Emergency Response Team (CERT) 2.2 Establish a shared situational awareness across government (Govnet); and the private sector 2.3 Develop a coordinated national cyberspace security response system to prevent, detect, respond to and recover from cyber incidents; 2.4 Establish focal points for managing cyber incidents that bring together critical elements from government, law enforcement agencies, infrastructure operators and internet service providers to reduce both the risk and severity of incidents; 2.5 Participate in watch, warning and incident response information sharing mechanisms; 2.6 Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.
3.0 Develop government, civil, and private industry collaborative relationships that work to effectively manage cyber risk and to protect cyberspace.	3.1 Provide a mechanism for bringing a variety of perspectives, expertise, and knowledge together to reach consensus to enhance security nationally; 3.2 Include industry perspectives in the earliest stages of development and implementation of security policy and related efforts; 3.3 Encourage private sector groups from different critical infrastructure industries address common security interests collaboratively with government; 3.4 Bring together the private, civil and public sectors in trusted forums to address Common cybersecurity challenges;

	3.5 Encourage cooperation among groups from interdependent organizations and agencies; 3.6 Establish cooperative arrangements for incident management between Government and various groups.
4.0 Promote a national culture of cyber security consistent with United Nations General Assembly Resolutions 57/239 entitled “Creation of a global culture of cyber security”; Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies and 58/199 entitled “Creation of a global culture of cyber security and the protection of critical information infrastructures”.	4.1 Implement a cyber security plan for Government operated systems; 4.2 Implement cybersecurity awareness programs and initiatives for users of systems and networks; 4.3 Encourage the development of a culture of cyber security in business enterprises; 4.4 Support outreach to civil society with special attention to the needs of children and individual users; 4.5 Promote a comprehensive national cybersecurity awareness program so that all stakeholders - business, the general workforce and the general population - secure their own parts of cyberspace; 4.6 Develop awareness of cyber risks and available solutions; 4.7 Enhance science and technology (S&T) and research and development (R&D) initiatives; 4.8 Review existing privacy regime in accordance with the digital environment; 4.9 Make digital literacy and IT security a priority in higher education; 4.10 Revise organizational security policy and improve the use of existing security tools; 4.11 Integrate work in higher education with the national effort to enhance digital literacy and strengthen critical infrastructure; 4.12 Improve collaboration between higher education, industry and Government.
5.0 Deter Cybercrime	5.1 Enact and enforce legislation relating to cyber security, cybercrime and data protection; 5.2 Build capacity of policy makers, regulatory staff, law enforcement and prosecution authorities; 5.3 Build local judicial capacity.

3.4 Critical Online Services

Liberia's call to Action is a proactive initiative that seeks to secure all spheres of its digital space. Foremost in this strategy are the need to protect critical online services including the following:

A. Online commercial and financial services
B. Online Government services
C. Online Revenue information services
D. Online protection of Big Data
E. Protection of Child online services
F. Protection of utility services online
G. Online counter measures on human trafficking and money laundering

This national cybersecurity strategy has illustrated that Cyber security is a component of the national security strategy. The protection of Liberia's borders and the maintenance of law and order is a function of national security. Since cybercrime is cross cutting and is committed with the objective of causing harm, a culture of cyber security that seeks to educate, protect and defend national cyberspace will be promoted in an effort to build a secure cyberspace.

4.0 Framework

Developing and implementing a comprehensive national cybersecurity strategy requires the true appreciation of issues and scope of work that must be executed. In this strategy the issues and scope of work cover seven critical areas. They are as follows:

1. **Governance**
2. **Incident Management**
3. **Capacity Building**
4. **Culture**
5. **Legislation**
6. **Collaboration, and**
7. **International Co-operation**

4.1 Governance

Governance plays a very critical role in making a national cybersecurity strategy to achieve its objectives. It is the framework that provides the structure through which the objectives of the nation regarding cybersecurity are set. It also provides the means of attaining those objectives and establishes how performance is monitored. Its ultimate goal is to further the public good. Cybersecurity efforts should effectively address the dynamic nature of threats to cyberspace.

An overarching governance framework is therefore required to effectively coordinate and manage a comprehensive cyber security strategy. In this regard, the Governance Framework is required to guide and coordinate all activities related to Liberia's national cybersecurity program. The governance layer includes the following:

1. The National Council on Cybersecurity (NCOC) - this shall be the body with the authority to set high level objectives and agenda for national cybersecurity programs.

It shall comprise

A. Ministry of Justice
B. National Security Advisor
C. Ministry of ……

2. It shall be chaired by the National Security Advisor to the President
3. The National Council on Cybersecurity (NCOC) will have responsibility for developing the implementation plan for the Cybersecurity Strategy 2019-2024, which will take into consideration the specific development plans of the relevant government agencies and identify concrete actions and the required budget and financing to achieve the objectives of the strategy.
4. The NCOC will develop a system of security measures to ensure national cybersecurity that addresses all the systems and platforms used for the provision of critical information services and provides for action plans for responding to cyber-attacks and the rapid recovery of damaged information systems. It will also specify the course of actions to be taken in the event of cyber-attacks that jeopardize national CII and the counter measures to be taken immediately at both the national and international levels.
5. The NSA shall be the agency to monitor the implementation of the national cyber security strategy; it shall provide situational awareness information, collect and analyze data on cyber security issues. It shall also coordinate and or manage the following core functional areas of cyber security:
   - Development and implementation of management frameworks for all functional areas;
   - Supervise Incident response and management;
   - Collaborate with the Liberia National Police to carry on Cyber forensics and investigations
   - Ensure that all measures are in place to support the Critical Information Infrastructure Protection (CIIP) and Critical Infrastructure Protection (CIP).

The protection of Liberia's cyberspace is a shared responsibility for all stakeholders. Each actor has a unique role to play and at the same time has a shared responsibility with other stakeholders as a way to consolidate the effectiveness of the security chain. This is the ultimate goal of the governance process.

4.2 Incident Management

The Incident Management Team (IMT) has the responsibility to deter and respond to cyber threats, and maintain the confidentiality, integrity and availability of critical national infrastructure and deter cybercrime as a function of Liberia's readiness to secure its cyberspace.

4.2.1 Membership of the Incident Management Team

Membership of IMT shall be determined. Liberia's national Cybersecurity Strategy shall facilitate, promote and strengthen national commitments to regional and global partnerships in fighting cybercrime.

4.2.2 National CERT

Liberia shall establish a national Computer Emergency Response Team (CERT) to ensure efficient response to security incidents within our cyberspace. An effective CERT response capability is essential to monitor, deter and appropriately respond to threats in Liberia's cyberspace. Liberia's National CERT shall be empowered through political will and the support of the Government of Liberia and its development partners to develop the necessary competencies and other capabilities.

4.2.3 National Incident Response Plan

To have an effective incident management portfolio, there shall be a National Incident Response Plan (NIRP). The plan shall define and establish procedures for incident response that will focus on incident classification and its severity. The plan shall ensure coordinated emergency response protocols, among others and it will govern both the national and sectorial CERTs.

4.2.4 Composition of the Technical Working Group

A subsection that defines the technical working group that comprises the IMT shall be developed

4.2.5 Other CERTs

All key national information infrastructures and institutions operating in the public and private sectors shall have a preventive mechanism for monitoring their system against cyber threats and cyberattacks. Such other CERTs shall be integrated into the national CERT to consolidate coordination. This level of system integration will facilitate effective analysis and detection of attacks making use of alert notification and other such indicators.

4.3 Capacity Building

Liberia has a low level of specialized cybersecurity skilled personnel required for driving national cybersecurity capabilities and empowerment. Without addressing this need, the national cybersecurity strategy cannot be effectively implemented since cybersecurity skills shall be required at every level of the implementation of the strategy. From infrastructure to human expertise dimension, capacity is required. A concerted national effort shall be exerted to develop core competencies and skills necessary to manage cybersecurity nationally. As such, partnerships shall be developed with the academic community to achieve this objective.

4.3.1 Liberia's Readiness

Intervention to develop Liberia's capacity in support of its readiness to secure its digital cyberspace shall include infrastructure, technical and procedural capacity. Infrastructure will address the network setup; technical will address the skill requirement on a continuous basis while procedural will cover judicial officers to enable them build their expertise and facilitate understanding of the dynamics of cybercrime. Cybersecurity skills development is a national priority and also a foundation for the achievement of national cybersecurity readiness.

The dividend for capacity building include the following:

- To build a critical mass of national professional with skills that shall be essential in manning our cyberspace;
- To establish efficiency levels critical to the central coordination activities of CERT;
- To help build an enlightened cyber culture based on professional training and capacity building in cybersecurity towards promoting common understanding on cybersecurity challenge.
- To elevate Liberia from a country with lack of cybersecurity capability to one with robust cybersecurity professional skills, producing secure local content under the expertise of its world class professionals to establish a national footprint in the digital space.

Lack of adequately skilled personnel is a major vulnerability, and operating a national cybersecurity program within this context will constitute a major risk to the nation, therefore the capabilities, skills and expertise of personnel charged with the responsibility of defending our presence in cyberspace will be periodically assessed, regulated and recommendations made to address identified gaps.

4.3.2 Operators and Owners

Owners and operators of infrastructure and Big Data services in Liberia's digital space shall identify vulnerabilities and design measures on how to address those vulnerabilities. Areas of interconnection that promote the interdependencies of system must be prioritized as well as the provision of redundancy programs to mitigate risks. Owners and operators of critical infrastructure shall consider the following approach in their preparedness towards enhancing the strategic readiness for the protection those critical infrastructure:

- Prevention and Early Warning Strategy
- Detection Strategy
- Reaction Strategy
- Crisis Management Strategy

4.4 Culture

Liberia shall endeavor to inculcate a culture that supports safe cybersecurity environment. It shall provide public education and facilitate how other stakeholders operating in Liberia's digital space shall contribute to building a safe and secure cybersecurity culture.

4.4.1 Building the Culture with other Players

Liberia shall ensure that all government institutions, corporate businesses, other organizations and individual owners and users of information technologies are aware of relevant cybersecurity risks and preventive measures that must be taken to prevent those risks. While government shall continue to encourage investment in this sector those who are making the investment should be cognizant of the threats and assume responsibility to secure their infrastructure from threats by taking steps to enhance the security of those technologies in line with United Nations General

Assembly Resolution 57/239. The coordinating role of Liberia's National CERT is geared towards achieving this objective.

4.5 **Legislation**

The reliance to deter cyber criminals and cyberattacks is the law. Liberia shall enact a cybercrime law that broadly deals with issues of cybercrimes and cybersecurity. Such law shall take into consideration global, continental and regional benchmarks in domesticating the objectives of the Budapest Convention under the ITU, the Malibu Conventions under the African Union and the ECOWAS Cybercrime Acts. Common across these instruments is the compelling need for each member country to establish a national regime consistent with global goals to fight cybercrimes. Liberia shall create the necessary legal and regulatory frameworks in fulfilling these objectives.

4.6 **Collaboration**

A public-private/civil society partnership is essential in securing Liberia's cyberspace. The GoL will partner with the private sector and civil society in the development, validation and implementation of its national cyber security strategy. Cooperation will be facilitated, through information sharing, participation in technology fora and research and analysis, to provide input for the development and dissemination of best practices for cyber security in Liberia.

Private enterprises, including Internet Service Providers (ISPs), have an important role in securing cyberspace as they own major networks and computer systems. These entities will be encouraged to evaluate the security of those networks that impact the security of Liberia's critical infrastructure. Liberia shall continue to value collaboration with all players as through collaboration there is a culture of sustained engagement on cybersecurity matters which will improve the chances to safeguard critical information infrastructure and nurture national cybersecurity readiness for the good of the society.

4.7 **International Co-operation**

The strategy on National Cybersecurity situates the National CERT as a structure to implement enforcement against cyberattacks. As Liberia seeks the partnership and cooperation of international and multilateral organizations, friendly governments and development partners, it is doing so to consolidate gains made at home in its readiness to improve its digital space.

References:

AU 2015, AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, Malibu

Government of Kenya 2014, National Cybersecurity Strategy, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf

ITU 2018, ITU Guide to Developing a National Cybersecurity Strategy, Strategic Engagement in Cybersecurity, Place des Nations 1211, Geneva 20 Switzerland Internet: www.itu.int

Nigeria 2014, National Cybersecurity Strategy, A Roadmap for Nigeria Cybersecurity Industry, https://www.cert.gov.ng/file/docs/NATIONAL_CYBESECURITY_STRATEGY.pdf, Federal Republic of Nigeria, Abuja

Annex – Organization Chart to be developed