

# **NATIONAL CYBERSECURITY POLICY**

## **FOREWORD BY THE NATIONAL SECURITY ADVISER**

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming our economy and security posture more than ever before, creating opportunities for innovations and the means to improve general welfare of the citizens. It is transforming many countries' growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas.

However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security. Sensitive data, networks and systems that we now trust can be compromised or impaired, in a fashion that detection or defence can be hard, thus undermining our confidence in a connected economy.

The Federal government is not unmindful of the diversity of implications of the nation's risk exposure in cyberspace, hence we have put in place cohesive measures towards addressing national risks effectively now and in the immediate future. Furthermore, the government has recognized that for Nigeria and its citizens to continue to benefit from the full potential of information and communication technology revolution, we must take the cyber-risks seriously. It is on this premise that we are determined to confront the threats, uphold and support the openness of the cyberspace as well as balance security with respect to privacy and fundamental rights. If we fail to prepare now and act appropriately, we may be faced with future challenges that will be more complex to manage.

In this context, government has developed a common framework that aggregates our collective responses towards addressing the challenges. These are encapsulated in this National Cybersecurity Policy. It outlines the actions government and other players alike will take to lessen the risks and secure the gains of our continuous dependence on cyberspace. The policy recognizes three key approaches to a successful national cybersecurity program: public private sector partnership; multi-stakeholders engagement; and international cooperation.

Our collective vision is to see a Nigeria, where law enforcement agencies are empowered in tackling cybercrimes; businesses and citizens are creating wealth and conscious of what to do to protect themselves on cyber space. This requires raising awareness on the imperatives of cybersecurity readiness as a vital component of our lives, as no individual or organization in any sector is immune from the consequences of cyber threat. In addition, ensuring private and public assets online are secure and resilient; and threats to the nation's infrastructure and national security are proportionately dealt with.

It is in the light of the above that my office, in collaboration with other agencies of government and key actors from the private sector are championing the urgent need for comprehensive national cybersecurity programmes. It is my hope that the synergy already developed between the stakeholders drawn from different backgrounds will be sustained through all the implementation stages. My office will continue to explore common grounds around which we can sustain this collaboration on cybersecurity for the common good of our country.

We shall keep all channels open for close monitoring and evaluation of the implementation of this policy, which shall be due for comprehensive review in another five years. My office shall facilitate regular collation of feedback from stakeholders that will enhance periodic review of the process.

I therefore wish to express my appreciation to the cross section of contributors and stakeholders, including professional bodies, corporate leaders and captains of industry who have contributed to our efforts towards creating an enduring safer digital environment for our dear country.

M. S. DASUKI CFR.

National Security Adviser

December 2014.

# TABLE OF CONTENT

FOREWORD BY NATIONAL SECURITY ADVISER.....

TABLE OF CONTENT.....

EXECUTIVE SUMMARY.....

## PART ONE: INTRODUCTION

1.1 Background.....  
1.2 Global Cybersecurity Context.....  
1.3 National Cybersecurity Threat.....

## PART TWO: THE NATIONAL DOCTRINES

2.1 Doctrine on Cyberspace.....  
2.2 Doctrine on Cyberspace Critical Assets & Infrastructures.....  
2.3 Doctrine on Cyber-Risk Exposure.....  
2.4. Doctrine on Cyber Security.....

## PART THREE: NATIONAL SECURITY & CYBERSECURITY

3.1 Goals of National Security Strategy.....

## PART FOUR: NATIONAL CYBERSECURITY ROADMAP

4.1 National Cybersecurity Vision.....  
4.2 National Cybersecurity Mission Statement.....  
4.3 Policy Objectives.....  
4.4 Policy Mandates.....  
4.5 The Guiding Principles.....

## PART FIVE: NATIONAL PRIORITIES

5.1 Introduction.....  
5.2 Strategic Areas of Focus.....  
5.3 Strategic Approach.....  
5.4 National Expectation & Strategic Benefits.....

## PART SIX: PRINCIPLES ON INCIDENT MANAGEMENT & CERT ECOSYSTEM

6.1 Preparation.....  
6.2 Indications and warning.....  
6.3 Detection and Response.....  
6.4 Vulnerability Handling.....  
6.5 Artifacts Handling.....  
6.6 Collaboration.....  
6.7 Sector-based CERT.....  
6.8 Training, Research and Development.....

**PART SEVEN: PRINCIPLES ON CRITICAL INFORMATION  
INFRASTRUCTURES PROTECTION**

7.1 Introduction.....

7.2 Vision of Nigeria Critical Information Infrastructure  
Protection Plan (NCIIPP).....

7.3 Policy Objectives Specific to NCIIPP.....

7.4 Strategic Readiness Plan (SRP).....

7.5 The Critical Infrastructure Sectors.....

7.6 Coordination Policy specific to CIIP.....

**PART EIGHT : PRINCIPLES ON ASSURANCE & MONITORING**

8.1 Introduction.....

8.2 Focal Points.....

**PART NINE: PRINCIPLES ON NATIONAL COMMITMENT  
& GORVERNANCE**

9.1. Introduction.....

9.2 Nature of Commitment.....

9.3 Nature of Governance.....

9.4 National Legal Commitments.....

9.5 Regional Commitments & Governance.....

**PART TEN : PRINCIPLES ON ONLINE CHILD ABUSE  
& EXPLOITATIONS**

10:1 Introduction.....

10.2 Strategic Areas of Focus.....

**PART 11: MISCELLANEOUS PRINCIPLES**

## **EXECUTIVE SUMMARY**

The dawn of the Internet has transformed our society in exceptional ways by enabling economic growth and providing new means by which people connect, interact and collaborate with one another. The convergence of components of information and communications technology (ICT); advances in underlying technologies fuelling reduction in costs, suggest that accessing the internet will become increasingly inexpensive and stress-free in Nigeria. The implication is that more and more people in Nigeria and around the globe will continuously engage in cyberspace. As more ideas continue to drive the expansion of the cyberspace for improved advantage and profitability, more surprises are unavoidable.

While heralding the success of the Internet, there is also a challenge in identifying and curbing cyber threat inherent within its sphere. It is well documented that the Internet is being used as a vehicle to carry out criminal activity within and outside Nigeria's borders. These activities adversely affect the country's economy as well as individuals and organisations within Nigeria's physical territorial boundaries from a financial, reputational, security and privacy perspectives.

Where external threat actors such as foreign intelligence agencies, hackers and other online criminal syndicates are carrying out the activities, they can also threaten the national security posture, which includes the economic, political and social fabric of Nigeria.

This policy therefore sets out the strategic intent of the government in mitigating the country cyber risk exposure by prioritising our needs while focusing on key areas, curtailing escalation of cyber threats that are inimical to the national security posture and the Nigerian economic wellbeing. This policy is a vital response element for safeguarding the nation. It helps to enlighten the citizens on the components that are to be used to empower the nation to understand, respond and collectively deter cyber threat activities. The policy outlines the doctrinal framework and guiding principles for achieving our roadmaps through a coordinated effort of all stakeholders in the country.

December 2014.

## **PART ONE**

### **INTRODUCTION**

This part sets out the overview of the Nigeria's National Cybersecurity Policy process and provides a background of Nigeria's cybersecurity status in relation to the global context. It also provides the rationale for the institution of a National Cybersecurity Policy.

#### **1.1 Background:**

Vision 2020 envisages improved socio-economic activities in Nigeria through the use of Information and Communication Technology (ICT). Similarly, recent developments in telecommunications and Internet expansion occasioned by introduction of undersea fibre optics, has resulted in improved use of the Internet for social and business activities in Nigeria. The country is operating progressively and actively in cyberspace.

Cyberspace has become an essential component of 21<sup>st</sup> century activities. As critical and non-critical activities are increasingly migrating to cyberspace, globalisation and the increasing interdependence of nations has also put significant pressure on nations to continuously look for ways of ensuring that the domain remains safe for players utilising it for social, economic and development purposes.

The purpose of the national cybersecurity policy is multifaceted. It considers the versatile landscape, the various stakeholders involved, and the threats posed by individuals and groups out there which take an undue advantage of users. Similarly, measures necessary to address national challenges come from an articulated approach, which must take into consideration the peculiarities and international commitments of the country.

## **1.2 Global Cybersecurity Context**

Cyberspace has become an indispensable global domain coming after Land, Sea, Air, and Space as number five. Increasingly, nations are depending on information and communications infrastructures in governing societies, conducting business, exercising individual rights on interactions and freedom of communication.

Cyberspace is open for diverse engagements. In contrast to land, air, sea and space, cyberspace poses unique difficulties in terms of the Non-boundary and universal nature of its networks. It does not recognize the conventional rules-based international systems. State actors, organized syndicate criminals, insurgents and terrorists are exploiting cyberspace for dubious purposes.

The world is confronted with growing challenges of cyber threat that constantly challenge confidentiality, integrity and availability of cyberspace, all of which can affect the critical functioning of nation states, including Nigeria. Global connectivity, vulnerable technologies, and anonymous nature enable the spread of disruptive cyber-activities that causes considerable collateral damage to a country's national interests. Cybersecurity is, therefore, an international challenge, which requires international cooperation in order to successfully attain an acceptable level of confidence and trust at national and global levels.

## **1.3 Nigeria National Cybersecurity Threat**

Five key cyber threats have been identified and listed as posing significant challenges to Nigeria and inimical to national growth and security. They are:

- a) Cybercrime
- b) Cyber-espionage
- c) Cyber conflict
- d) Cyber-Terrorism
- e) Child Online Abuse & Exploitation

Activities classified under these unwholesome schemes that are taking place on the Internet or on using information systems, have impact on the level of risk exposure, resistance and protection of associated national critical and non-critical infrastructure.

These threats have serious implications for the nation's presence and active participation in the global ecosystem. Nigeria is therefore keen to secure and protect its cyber space in a coordinated and all-inclusive manner.

Government is striving to understand the emergent complex threat landscape and contending with the breadth and depth of cyber attacks, especially those affiliated with nation-states or organised crime.

Therefore, the protection, security, and sustainability of the nation's active presence in cyberspace are dependent on the country's readiness to articulate a strategic approach and engagement roadmap to secure the nation's cyberspace.

In 2004, the Nigerian government developed a framework for cyber security following recommendations by the Presidential Committee on Illegal Online Activities. The strategic framework deals with the overall goal of setting a clear direction, coordination of the nation's engagements in cyberspace, as well protect and defend the national interests and the sovereignty of Nigeria.

This culminated into the establishment of the Cyber Security Focal Point at the Office of the National Security Adviser (ONSA). Various activities and initiatives have been taken by ONSA in collaboration with various stakeholders towards ensuring security of the country's presence in cyberspace.

# **PART TWO**

## **THE NATIONAL DOCTRINES**

Part 2 describes Nigeria's cybersecurity doctrines in specific terms. It also provides basic understanding of the doctrinal frameworks within which they are defined.

### **2.1 Doctrine on Cyberspace:**

2.1.1 Cyberspace is an interdependent network of critical and non-critical national information infrastructures, convergence of interconnected information and communication resources through the use of information and communication technologies. It encompasses all forms of digital engagements, interactions, socializations and transactional activities; contents, contacts and resources deployed through interconnected networks.

2.1.2 Cyberspace is recognized as a domain for non-critical and critical national functions such as economic development, trade and commerce, social interactions, communication, medical and health, government operations, national security and defence.

### **2.2. Doctrine on Cyberspace Critical Assets & Infrastructure:**

2.2.1 The operation, sustaining and survival of critical national functions is anchored on a safe and secure national critical information infrastructure, robust policies and processes with skilled manpower to manage such critical infrastructure. These complements of empowered people, processes and systems are fundamental to the cardinal objectives of Nigeria's National Cybersecurity Policy and its abiding principles.

## **2.3 Doctrine on Cyber-Risk Exposure:**

2.3.1 National functions rely on interdependent networks of critical information infrastructures for confidentiality, integrity, availability and accessibility.

2.3.2 Interdependent network of critical information infrastructures do not exist in isolation of global networks, i.e. the cyberspace.

2.3.3 National functions are recurrently exposed to predictable and unpredictable risks in the cyberspace.

2.3.3 Any disruption of critical national functions as a result of their exposure to cyber risks, that compromise their confidentiality, integrity, availability and accessibility constitute a threat to the doctrines of National Security.

## **2.4 Doctrine on Cybersecurity:**

2.4.1 National provision of sustainable proactive measures mitigates, protects, and safeguards the nation from cyberspace risk exposures, including cyber-threat and vulnerability. An insecure cyberspace is inimical to the nation's sovereignty, national security and economic development.

## **PART THREE**

### **NATIONAL SECURITY & CYBERSECURITY**

#### **3.1 The Goal of National Security Strategy on Cybersecurity**

- 3.1.1 The fundamental aim of the National Security Strategy as enshrined in the National Security Policy framework seeks for a harmonized security strategy that will respond to the dynamism of the national security threat landscape.
- 3.1.2 One of such emergent national security threat landscape is national risk exposure and uncoordinated presence in cyberspace.
- 3.2.3 In the context of the immediate and future security challenges, instruments of Nigeria's National Cybersecurity Policy and National Cybersecurity Strategy are intended to manage security threats in cyberspace in line with the overall national security objective.

## **PART FOUR**

### **NATIONAL CYBERSECURITY ROADMAP**

#### **4.1 National Cybersecurity Vision:**

A safe, secured, vibrant, resilient and trusted community that provides opportunities for its citizenry, safeguards national assets and interests, promote peaceful interactions and proactive engagement in cyberspace for national prosperity.

#### **4.2 National Cybersecurity Mission:**

To foster harmonious, sustainable and integrated Nigeria's national cybersecurity readiness and coordination capacities towards addressing and mitigating the nation's cyber risks exposure in cyberspace.

#### **4.3 Policy Objectives:**

##### **4.3.1 Statement of Purpose**

The aim of this National Cybersecurity Policy is to chart a course towards an assured and trusted presence in cyberspace.

##### **4.3.2 Objectives**

The objectives of National Cybersecurity policy are stated as follows:

- i. To facilitate an effective legal framework and governance mechanism for Nigeria's presence in cyberspace and cybersecurity ecosystem.
- ii. To develop an information security and control mechanism for the protection and safety of Nigeria's national critical information infrastructure and its associated economic infrastructures operating in cyberspace.

- iii. To provide measures for the identification, monitoring, analysis, and evaluation of the national critical information infrastructure for maintaining Nigeria's active presence in cyberspace.
- iv. To develop a national cybersecurity assurance framework, compliance and enforcement administration.
- v. To develop a centralized national emergency readiness and incident management coordination capability.
- vi. To promote emergence of an appropriate legislative environment with respect to freedom of access to information, intellectual property, data protection and privacy rights.
- vii. To promote and engage cybersecurity innovations through research and development in partnership with industry and academic institutions.
- viii. To develop a national benchmark for regular statistical data and situational report on Nigeria's cybersecurity status.
- ix. To develop a framework for inter-agency collaboration on combating cybercrime and cybersecurity.
- x. To establish multi-stakeholder partnerships, cooperation and leadership advisory mechanisms for information sharing, intelligence gathering and coordinated response.
- xi. To promote the infusion of the culture of cybersecurity and promotion of adherence to principles, standards and guidelines in the country.
- xii. To develop a coordinated national awareness strategy, capacity building, and structured cybersecurity professional cadres across all national constituents.
- xiii. To develop national criteria for the development of cybersecurity manpower, identify baseline requirements, qualifications for

cybersecurity professionals and implement measures for certifications and regulations of cybersecurity skills, products, and services.

- xiv. To promote and strengthen Nigeria's national commitments to regional and global partnerships and cooperation on cybersecurity.
- xv. To facilitate institution of a unified National Strategy on Cybersecurity to provide guidance, initiatives and measurable action plan in the development, implementation, and sustainability of a national cybersecurity roadmap.
- xvi. To develop a national mechanism for the establishment of Nigeria's National Cybersecurity Coordination Center (NCCC) to serve as the focal point for cybersecurity incident monitoring and response; coordinate and regulate Sectoral Computer Emergency Response Team (S-CERT) and establishment of a National Digital Forensic Laboratory (NDFL) in the country.

#### **4.4 Policy Mandates:**

- 4.4.1 The National Cybersecurity Policy mandate is derived from a Presidential directive vested on the Office of the National Security Adviser in pursuant of the comprehensive National Security Policy and Strategies.
- 4.4.2 The Presidential order mandated the Office of National Security Adviser to establish cybersecurity structure within the Office of the National Security Adviser (ONSA).
- 4.4.3 The mandate of the cybersecurity structure among others is to develop a National Cybersecurity Policy and implement a National Cybersecurity Strategy for the country.
- 4.4.4 The Office of the National Security Adviser, therefore in exercise of its power authorized the institution of effective Nigeria's National Cybersecurity Policy and Nigeria's National Cybersecurity Strategy. These are parts of a

comprehensive National Security Policy framework based on the immediate and long-term national security risks mitigation strategy.

## **4.5 The Guiding Principles:**

4.5.1 The following guiding principles provide direction to the national approach to cybersecurity while simultaneously addressing critical areas of conflict.

4.5.2 These principles form the underlying philosophy of the country's response to the identified five cyber threats inimical to Nigeria's national security and interest:

### **i. General Principles:**

- The policy is taking cognisance of the borderless nature and global landscape of cyberspace.
- The policy measures to improve Nigeria's cybersecurity posture are adaptable to the dynamism of cyber threats and flexible legislative landscape.
- The policy measures are based upon national capabilities in identifying and managing cyber-risks with understanding of the underlying threats and vulnerabilities.
- Initiatives to improve Nigeria's cybersecurity posture must be anchored on stakeholder's coordination, cooperation and international collaboration.
- The policy recognizes the protection and safety of the nation's most critical assets i.e. its citizenry and vulnerabilities online, thus, the policy takes a stand against online child abuse and exploitation.
- The policy recognizes the need for a cybersecurity regulatory framework for the country through stakeholders' collaboration.

**ii. Specific Principles on Cybercrime and Proactive Measures:**

- Cybercriminals exploit the vulnerabilities of the nation's cyberspace. The rise of cybercrime has a negative socio-economic effect on the nation's integrity and the citizens.
- It is cardinal principle of this policy to put in place appropriate proactive measures towards preventing threats to the nation's cyberspace while mitigating the impact on its citizens.
- The proactive policy measures recognized global principles on cybersecurity and will work towards addressing the following objectives:
  - a. Technical measures to identify, monitor, detect, prevent, respond and investigate cybercrime.
  - b. Legal measures to deter, investigate, prosecute, and punish cybercrime
  - c. Economic measures to provide appropriate assistance to combat cybercrime.
  - d. Social measures and capacity building aimed at raising awareness among Nigerian nationals towards reducing the nation's cybersecurity exposure footprint.
  - e. Fostering of international commitment and cooperation against cybercrime.

**iii. Specific Principles on Cyber-espionages and Comprehensive Measures:**

- The Cyber-espionage comprising economic and military espionage constitute critical cyber threats that can compromise national security and stunt economic growth.
- An abiding principle of this policy is to put in place appropriate comprehensive measures involving multidimensional engagements of

military and civil security collaborations, national and international security cooperation to detect and deter cyber-espionage.

**iv. Specific Principles on Cyber Conflicts, Cyber terrorism and Integrated Containment Measures:**

- At the centre of this policy lays the principle of integrated containment of conflicts, violence and terror perpetuated against the sovereignty of the nation by agents and groups exploiting the borderless nature of cyberspace.
- It is the core principle of this policy to articulate integrated containment measures which focus on shared responsibilities and cooperation among all the state actors at the national, regional and global levels.
- This policy seeks to prevent and contain cybercriminal intents and related malicious acts inimical to the national dignity, security and economic interests of the country.

**v. Specific Principles on Child Online Abuse & Exploitation and Counter-measures:**

- Social media has become a vital attractive channel and tool for social interactions and productive engagements. The open and transparency nature of cyberspace have been exploited for good causes and malicious intents.
- It is the cardinal principle of this policy to harness counter-measures through a legislative framework, policy and strategic actions, including international cooperation, to address cyber abuse and online exploitation of the Nigerian Children.

**vi. Specific Principles on Balancing Security, Data Protection, Privacy Rights, Freedom of Expression and Information sharing:**

- The policy shall promote full trust and protection of economic benefits of cyberspace by sustaining balance between citizen's expectations on freedom of information and privacy, and government responsibilities on data protection.
- The Policy shall ensure that conflicting issues of data protection and information sharing will be addressed through appropriate cybercrime legislative frameworks that will include socialization of legislations.
- The policy is committed to provide appropriate data governance measures and an effective data protection and privacy regime, where data owners and their processors shall have their obligations to protect citizen's personal data, as well as operate within the law when collecting, protecting and processing such information.

**vii. Specific Principles on Freedom of Expression & Political Stability:**

- The policy shall respect the free flow of information under secured and trusted environment that satisfies the security needs of government, citizens and private sector.
- The policy shall ensure commitment to default position where Nigerians and individuals within its borders shall be free to express their opinions without fear or reproach when using online media.
- The policy shall ensure that where individuals, organization's or corporations' expressions undermine the national security posture and or political stability of the nation, in such instances, individuals, organizations or corporations making such expressions shall be prosecuted under new legislations, which will be addressed by the cybercrime legislative framework.

**viii. Specific Principles on Privacy and Lawful Interception:**

- In order to address the conflicting issues of privacy and lawful interception, the policy shall ensure commitment to the default position where Nigerians and other nationals communicating within its borders shall be allowed to

communicate without having their communications intercepted or eavesdropped on.

- This right to privacy shall only be removed where individuals are reasonably suspected of committing a crime or are involved in activities that threaten or undermine the nation's national security posture.

**ix. Specific Principles on Public and Private Sector Partnership:**

- The policy recognizes the important role of private sector in cyberspace and its massive investments in the provision of critical resources, intellectual assets and management of critical national information infrastructure.
- The policy recognizes the cyber risk exposure of critical infrastructures, which leads to Industries increasingly becoming the primary target of cybercrime, cyber espionage, and most recently, serious cyber attacks.
- The policy is committed to building trusted channels for strategic partnerships with the private sector through public-private partnerships and multi-stakeholder engagement measures.
- It is strategic intent of this policy to facilitate cross-sector harmonization, development and application of a common regulatory framework towards entrenching a cohesive cybersecurity response. This is to improve cybersecurity across the critical information infrastructure.

**x. Specific Principles on Sustainable National Awareness, Advocacy and Capacity Building:**

- The policy seeks to improve the country's cybersecurity posture. Therefore it is the abiding principle of this policy to provide measures on sustainable national awareness, advocacy and capacity building

across various spectrums, encompassing government and private sectors institutions, security and law enforcement agencies as well as individual citizens.

**xi. Specific Principles on Cybersecurity Innovation & Manpower Development:**

- The policy recognizes the need for national expertise, local skills development, and harnessing of local potentials through coordinated national mechanism, towards addressing fast changing cyber threat and the dynamism of the nation's cyber risk exposure.
- This includes encouraging knowledge sharing and transfer, creativity and innovation necessary to respond to such changing cyber threat landscape.

**xii. Specific Principles on Cloud Computing Security, National Data Security Management & Hosting:**

- The policy recognizes cloud computing as an evolving sub-domain of cyberspace. The policy will harness and align cloud computing security frameworks and guidelines in line with national interest and economic protection needs of the country.
- Within the context of national security, the policy maintains a position that the nation and its organizations do not transfer hosting of critical national data to countries that do not have effective data protection and privacy regimes.
- The policy recognizes the evolving nature of the country's capability on local data hosting infrastructure and management services. Thus, the policy will facilitate country capability in partnership with stakeholders.

**xiii. Specific Principles on Cyber-Physical Infrastructures:**

- The policy seeks to facilitate a regulatory framework that would secure the most critical cyber-physical systems, which control core

infrastructure whose failure could adversely disrupt economic activity and national security.

**xiv. Specific Principles on Organizational Cybersecurity:**

- The policy supports cybersecurity capability of the nation's business entity, thus enabling businesses to work with government, to dynamically evaluate measures as appropriate towards addressing threat and vulnerability.

**xv. Specific Principles on Multi-Stakeholders Engagement:**

- The policy recognizes shared responsibility on cybersecurity and multi-stakeholder nature of cyberspace. Therefore, the policy would promote National Cybersecurity Multi-stakeholder Intervention to support effort on a cohesive security incident response and management.

**xvi. Specific Principles on International Commitment & Governance:**

- The policy is committed to abide by the national legal framework, regional jurisprudences, international agreements, facilitating bilateral co-operations, multilateral partnerships, cybercrime conventions and treaties on cyberspace and cybersecurity.
- The policy would seek to promote international alignment and harmonization on global cybersecurity.

## **PART FIVE**

### **NATIONAL PRIORITIES**

#### **5.1 Introduction:**

This part addresses actionable *statement of purpose principles* in the strategic areas of national priority. It defines critical areas of focus for policy actions towards a coordinated cybersecurity engagement.

#### **5.2 Strategic Areas of Focus**

##### **5.2.1 Legal Framework**

- i. The Government has the responsibility of taking legal and regulatory actions to improve and update its federal and state laws to combat cybercrime.
- ii. This policy recognizes and supports various enacted laws administered by different government agencies that impact on cybercrime countermeasures and cybersecurity.
- iii. It is the policy of the government to develop an appropriate Cybercrime legal Framework to provide legal response to tackle, prosecute and deter cybercrime activities in Nigeria.
- iv. The Cybercrime Legal Framework will have processes to ensure that it is constantly reviewed so that it can enact or amend laws that are effective in meeting the fast paced changes and technological developments in the cybercrime environment.
- v. The policy shall facilitate and promote a set of related legislations, which have impact on the nation cybersecurity strategy

and engagement in cyberspace.

- vi. The Cybercrime Legal Framework will adopt international conventions and best practices. It shall include international cooperation and their law enforcement agencies to tackle cybercrimes that are committed inside the nation's borders with impact on individuals and organizations outside of Nigeria. It will also address activities emanating from outside of Nigeria which affect individuals and organizations in Nigeria.
- vii. The framework will use appropriate cooperation and collaboration platforms to participate in international fora to allow government and citizens of Nigerians to have a voice in decisions that could adversely affect their participation on the Internet. Such discussions include but are not limited to Internet Protocol Address profiling.
- viii. The Cybercrime Legal Framework will reform substantive and procedural criminal laws in Nigeria to address the phenomenon of cybercrime.
- ix. The Cybercrime legal Framework will establish legislations to combat cybercrime. New legislations will aim to meet the changing cybercrime landscape and as a minimum consist of the following legislations to compliment already existing criminal laws: Anti-Spam, Child Online Protection; Child Pornography; Cookies; Computer Misuse; Cyber Blackmail; Cyber bullying and Harassment; Cyber Espionage; Cyber Terrorism, Digital Evidence and Preservation; Data Protection; Data Retention; Activism; Identity Theft; Information Security; Intellectual Property Rights; Lawful Interception; Online Fraud; Privacy; Tribalism and Xenophobia; Software Piracy; Security Breach Notifications; Unauthorized System Interference among others.
- x. It is the policy of the Nigerian Government as part of this legal framework to ensure capacity building of the judiciary, lawyers and regulatory bodies towards guaranteeing that Nigeria has appropriately trained and skilled resources to adjudicate and advise on the complex issues that will arise from prosecuting cybercrime.

- xi. The policy proposes for an advisory and assistance mechanism to the legislative authority on the appropriate time to enact changes to cybercrime laws.
- xii. It is the policy of the Nigerian Government that cybersecurity and cybercrime legal education be adopted into the syllabus of institutes of higher learning to ensure that new entrants to the industry have basic knowledge and understanding of the issues relating to cybercrime and cybersecurity.

### **5.2.2 Structures & Coordination**

- i. It is required that there shall be a unified coordination of national cybersecurity policies and strategies in the country. This coordination requires a national structure to facilitate national cohesion at strategic and tactical levels.
- ii. This policy, therefore, provides for the setting up of a National Cybersecurity Structure, which will be the National Cybersecurity Coordinating Center and the international focal point for cybersecurity in the Office of National Security Adviser (ONSA).
- iii. The Nigeria's National Cybersecurity Coordinating Center shall provide the following cybersecurity responsibilities;
  - Provide national cohesion and intervention at operational and strategic levels through the implementation of a national cybersecurity strategy.
  - Provide coordination and implementation of cybercrime counter-measures for law enforcement and security agencies.
  - Supervise, coordinate and regulate sectoral cybersecurity measures.
  - Develop and provide collaborating mechanisms and counter-measures on online abuses and exploitations of Nigerian children.

- Provide mechanism for information sharing, intelligence data gathering and surveillance of national cyberspace, which must be within national jurisprudence.
- Develop and provide mechanisms for national cybersecurity assurance; cybersecurity emergency readiness; and incident responses capabilities.
- Develop a national laboratory, research and innovation capability for digital forensics.
- Develop national technical standards on cybersecurity framework, provide guidelines on compliance, training and capacity building for all military and non-military public institutions, institutions, including the Judiciary and legislature.
- Perform regular cybersecurity exercise, national cyber-risk exposure assessment, determine needs and provides appropriate responses for mitigations.
- Develop, implement and facilitate a national mechanism on public awareness, cybersecurity education, advocacy on cyber safety and culture of cybersecurity for the country
- Provide a national technical focal point on cybersecurity for regional and international collaborations and partnerships.
- Provide and facilitate mechanisms for cybersecurity skill development, innovation, research and development in partnership with stakeholders.
- Provide all other cybersecurity functions that safeguard national interest on cyberspace.

**iv.** The policy recommends the setting up of National Advisory Council on Cybersecurity (NACC) whose membership should reflect public-private

partnership and multi-stakeholder nature of the guiding principles of this policy.

- v. The NACC will provide the following responsibilities:
- Guidance and advisory to the National Security Adviser on policy and other matters relevant to cybersecurity and cybercrime countermeasures.
  - Facilitate multi-stakeholder engagements as well as public and private sector collaborations on cybersecurity.
  - Promote cooperation and partnership among all government institutions.
  - Provide other functions that may enhance the capability of NCCC towards achieving trust and confidence in the country.

### **5.2.3 Monitoring & Assurance**

- i. The nation's capabilities to provide assurance, i.e monitoring, compliance and audit, on various cyber security measures, plans and programs depend largely on her ability to perform monitoring, evaluations, assessments and reviews of cybersecurity programs implemented to ensure that they meet national expectations.
- ii. This policy seeks harmonized framework for relevant international standards and technical measures that respect national priorities that promote and protect critical national interests.
- iii. Such framework must recognize national innovations, promote national cohesion and reposition the country for global trust and confidence in its digital economic agenda.
- iv. The following shall serve as the basis for guiding strategy on assurance, monitoring and compliance in the country:

- A risk-management based and technology neutral approach shall be adopted in performing assurance activities.
- Continuous improvement in the nation's security posture shall be an objective underpinning assurance activities and recommendations.
- All cyber security initiatives shall be assessed for conformity with relevant laws, harmonized frameworks, cost effectiveness and the ability to provide a secure and a safe cyberspace that contributes positively to the nation's growth.
- A continuous monitoring approach shall be used to assess, security trends, threats and risks that face the nation's cyberspace.
- Regular security audits shall be performed to determine the status of implemented cyber security controls and general security posture of the nation's cyberspace.

#### **5.2.4 Critical Information Infrastructure Protection (CIIP)**

- i. It is the policy of the Government to develop national guidelines and criteria for profiling information infrastructure with a strategic intent of determining, identifying, and classifying critical national information infrastructure.
- ii. This policy will enable a mechanism for addressing vulnerability of nation's Critical Information Infrastructure.
- iii. This policy seeks proactive security measures and controls throughout all government institutions towards addressing vulnerabilities and related security gaps within internal information systems, processes and users.
- iv. Such measures should adapt to the national cybersecurity standards and guidelines as provided for in the National Cybersecurity Strategy.

- v. The dynamism of cyber threat and the adverse impact on Critical Information Infrastructure will be addressed through continuous engagement of stakeholders from organized private sector.

#### **5.2.5 Unified Measures**

- i. The policy shall harness, harmonize and prioritize various frameworks to address the following critical areas of national cybersecurity agenda;
  - Computer Incident Security Response
  - Online Child Abuse & Exploitations
  - Nigeria Internet safety.
- ii. The framework for the establishment of computer incident security response shall be in harmony with international best practices, taking into consideration various international conventions, standards and guidelines.
- iii. The policy shall address Online Child Abuse & Exploitations from the following approaches; law enforcement and security countermeasures; legal framework; multi-stakeholder intervention; and international cooperation. The policy seeks to bridge these approaches towards cohesive measures.
- iv. The policy will promote multi-stakeholders' initiatives and relevant framework for safeguarding Nigeria community and citizens' engagement in cyberspace.

#### **5.2.6 Cybersecurity Skills & Empowerment**

- i. The policy prioritizes the strategic needs to develop national manpower and skill development in cybersecurity knowledge and education across the sectors.
- ii. The dynamism of cyberspace, cyber threat and national vulnerability requires structural and continuous capacity building, cybersecurity skills development and empowerment

framework where the nation can effectively deploy her nationals to safeguard her national interests.

iii. This policy provides for the following frameworks for the development of cybersecurity skills in the country and for law enforcement and security agencies specifically.

- Setting up of a cybersecurity institute in partnership with stakeholders.
- Development of minimum set of standards for the regulation and coordination of professional practices in information security.
- Development of national cybersecurity curriculum framework and specific requirements that cuts across law, social sciences, information and communication technology, information assurance, management and cyber-diplomacy.
- Establishment of operational cadres for cybersecurity professionals in Military and non-military security agencies, government institutions, department and agencies.
- Enabling private sector support in cybersecurity professional development relevant to the nation's economic and national security interests.
- Development and adoption of national mechanism for the infusion of cybersecurity knowledge and culture at all levels of education.

#### **5.2.7 National Advocacy for Stakeholder Engagement**

i. National advocacy for stakeholders' engagement is the critical success factor of National Cybersecurity Policy which is anchored on trust, transparency and confidence building in the policy actions of government.

- ii. This policy will harness its comprehensive approach, guiding principles and all the three modes of engaging different levels of stakeholders using the following principles:
- Coordination within government towards achieving a unity of purpose across the different levels of government, especially within federal government and between states and local government administrations.
  - Cooperation with local non-governmental stakeholders including organized and non-organized private sector, formal and informal sectors which are central to national cybersecurity issues. The policy will facilitate voluntary cooperation and harmonious relationship through formation of public-private partnership and multi-stakeholders partnership towards facilitating exchange of information on the development of new legislation and regulation between stakeholders.
  - Collaboration within the regional and international community, bilateral and multi-lateral institutions, multi-national corporations, and global cyberspace governing bodies. The policy recognizes various contributions of international discourse on Internet governance, policies and management of cyberspace critical resources and contributions of global institutions.

#### **5.2.8 Research & Development in Cybersecurity Innovation**

- i. Cyberspace is a dynamic domain providing opportunities for global competitions driven by innovations while at the same time, cyber threats continue to evolve in complexity and gravity.
- ii. The policy will promote innovation in cybersecurity towards the development of security tools and protection of information infrastructures.

- iii. The policy will stimulate government-industry-academia collaboration on cybersecurity research and development to prevent duplication of efforts and leveraging on collective capabilities.
- iv. The policy will facilitate national mechanism on cybersecurity research and development to help the country develop a process of transition from the current cyberspace infrastructure to a more resilient and secure platform. This is a critical imperative towards securing the nation's cyberspace.

### **5.2.9 International Synergy**

- i. It is the principle of this policy on cybersecurity to encourage active international synergy and participation in relevant international cyber security fora and multi-national agencies discourse on cyber threat and cyberspace.
- ii. The policy will promote the country's active participation in relevant international cyber security policy formulation, technical fora, hosting of national and international cybersecurity conferences that will facilitate the country's leading role in transnational cybersecurity measures.

### **5.3 Strategic Approach**

- i. The strategic approach to the development of an all-inclusive National Cybersecurity Policy requires taking a look at cyber security from national security risk and economic interest perspectives. Equally vital are perspectives from local and global stakeholders that are applicable to national peculiarities and that can help the nation to meet her national and international commitments.
- ii. The policy will consider past outcomes, submissions, and recommendations of various stakeholders meetings, fora, workshops and conferences.

- iii. The policy will further examine the basic decisions that must underpin national policy and strategy on cybersecurity, while identifying the national stakeholder groups that will work with the strategy.

#### **5.4 National Expectations & Strategic Benefits**

This policy offers the country unique opportunities of building a reliable and trusted connected community with the following strategic benefits;

- i. Global confidence in the nation's digital economy
- ii. Safeguarding of the nation's presence in cyberspace
- iii. Stakeholders confidence and trust in the nation's ICT sectors and infrastructures
- iv. National safety and protection of national critical Infrastructures
- v. Positive impacts on economic growth and enhances the nation's competitive advantage
- vi. Promotes national values, dignity, identity in cyberspace and improves national image
- vii. Stimulates foreign direct and indirect investment flows into country
- viii. Promotes a vibrant and safe environment for social interactions and e-commerce transactions.
- ix. Enables the country address emergent security challenges, builds the nation's capacity to detect, analyze, respond and manage cybersecurity incidents.
- x. Reduces prevalence of cybercrime activities while inducing safety and security consciousness among the public.

- xi. Assures the provision of a comprehensive national security strategy for immediate and future engagements; and
- xii. Consolidates the leading and functional roles of Nigeria at regional and global levels on matters relating to cybersecurity.

## **PART SIX**

### **PRINCIPLES ON INCIDENT MANAGEMENT & ECOSYSTEM**

#### **6.1 Preparation:**

- i. To ensure resilient national cyberspace, a coordinated incident management capability shall be required to manage cybersecurity incidents.
- ii. Nigerian Computer Emergency Response Team (ngCERT) mechanism shall be established and empowered as the focal point for all national cyber incident management.
- iii. The ngCERT mechanism shall be managed under the supervision of NCCC.
- iv. There shall be one national CERT. It shall function as a central coordinating unit under the NCCC to manage all cyber-incident activities within the national cyberspace that may affect national security.
- v. A National Incident Response Plan (NIRP) will be formulated towards achieving a coordinated emergency response strategy based on the National Security Policy.

- vi. The NIRP will integrate processes for monitoring with rapid response, and efficient resolution to mitigate impact to the security and the economic wellbeing of the nation.
- vii. The NIRP will be implemented and coordinated by ngCERT under the supervision of NCCC.
- viii. NCCC shall develop standards and guidelines in collaboration with relevant statutory federal government agency for the establishment and operations of sectoral CERT.

## **6.2 Indications and warning:**

- i. All key national information infrastructures shall have a proactive network monitoring system for effective monitoring and interception.
- ii. A centralised Cyber Emergency Monitoring System (CEMS) under ngCERT coordination shall be implemented to identify indicators for potential threats to the nation's cyberspace.
- iii. Based on the potential threat identified by the CEMS, alerts and warnings will be issued to various agencies and entities for rapid response and vulnerability patches.
- iv. All Internet service providers and internet exchanges shall interface with ngCERT for effective utilisation of a unified national alert and warning system to be established and maintained by the NCCC.

## **6.3 Detection and Response:**

- i. Incident detection and prevention mechanism is required for all critical information infrastructures.
- ii. Security incident without localised expertise must be escalated to the central coordinating unit for additional support as will be outlined in the NIRP.

- iii. For business continuity purpose, cybercrime incident occurring must be recorded, reviewed and resolved following an established incident management process as may be define in NIRP.
- iv. All Cybercrime incidents must be documented and reported to ngCERT.

#### **6.4 Vulnerability Handling:**

- i. Security assessment and audit shall be periodically required on critical national information infrastructure. It shall be carried out at a pre-defined interval and integrated into the National Incident Response Plan (NIRP).
- ii. There shall be provision for the documentation and archiving of all vulnerabilities and patches according to manufacturer's specifications. A national record shall be kept for review.

#### **6.5 Artifacts Handling:**

- i. The policy requires the development of national guidelines on digital evidence handling which shall be incorporated into the NIRP.

#### **6.6 Collaboration:**

- i. ngCERT shall be saddled with advocacy to promote trust within the national cyberspace.
- ii. All collaboration with regional and international CERTs shall be coordinated by ngCERT as the National Point of Contact (POC).
- iii. All sectorial computer emergency response team (CERT) shall be promoted and supported by ngCERT. Technical support and expertise will be provided as when required.
- iv. A national trust level classification shall be established to cater for different tiers of sectorial CERT.

#### **6.7 Sector-based CERT**

- i. Sector-based CERT shall be set up by the sector supervising regulatory body and or other coordinating body within a particular sector.
- ii. Sector-based CERT shall serve as a single point of contact (POC) for each of the specific sectors and coordinate incident response activities in the sector
- iii. Sector-based CERT shall promote trust and confidence among stakeholders under the specific sector.
- iv. Sector-based CERT shall facilitate information sharing and technology exchange with ngCERT.
- v. Sector-based CERT shall facilitate provision of criteria, measures, standards, guidelines and best practices for the sector in line with national cybersecurity measures.
- vi. Sector-based CERT shall undertake cybersecurity readiness, information security assurance and compliance administration for the specific sector.
- vii. Sector-based CERT shall operate in cooperation with the ngCERT towards achieving the common goal of securing the nation's cyberspace.
- viii. There shall be strengthening of relationship between Sector-based CERT and ngCERT
- ix. All sector-based CERT shall constitute national ecosystem, with proper identifications with specific roles and mandates.
- x. All members of the eco-system shall be coordinated, regulated and certified by ngCERT.

## **6.8 Training, Research and Development:**

- i. A localised approach shall be adopted to develop in-house technology and security tools for managing threats peculiar to the nation.

- ii.** NgCERT will provide training, requirements and national criteria to sectoral CERT for ease of operation and efficient and effective response to security incidents.
  
- iii.** NgCERT shall collaborate with sectoral CERT on research and development with the goal of fostering innovation in cybersecurity.

## PART SEVEN

### PRINCIPLES ON NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

#### 7.1 Introduction:

- i. It is the cardinal objective of this National Cybersecurity Policy to complement the efforts of the Federal Government of Nigeria on the existing plans and documents relating to safeguarding and protection of the nation's Critical Information Infrastructure.
- ii. The legislation on cybercrime and cybersecurity thus states that *The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.*
- iii. This policy recognizes that Nigeria's well-being depends largely on a secure and resilient critical national information infrastructure—the systems, assets and networks that underpin our national life.
- iv. Therefore, this policy details how the private sector will work with government in the identification and protection of critical infrastructure in order to manage risks and achieve resilience to national critical information infrastructure.

## **7.2 Vision of National Critical Information Infrastructure Protection Plan (NCIIPP)**

The country envisions an environment where physical and cyber critical infrastructure are secure and resilient, with vulnerabilities reduced and consequences minimised to acceptable tolerable limits, where threats are identified and dealt with in a coordinated response and recovery strategy.

## **7.3 Policy Objectives of NCIIPP:**

- i. Detect, identify, discourage, disrupt and prepare for threats and cyber hazards to Nigeria's critical information infrastructure
- ii. Reduce vulnerabilities of critical assets, systems and networks to deliberate, unintentional and natural threats.
- iii. Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur through advance planning and mitigation efforts to save lives and ensure prompt recovery of essential services.
- iv. Share important and actionable information among the critical infrastructure community in order to build awareness and provide a risk-informed decision making.
- v. Promotes learning and rapid revision of NCIIPP during and after incidents.

## **7.4 Strategic Readiness Plan (SRP)**

- i. The policy shall facilitate the development of a strategic action plan through a collaborative process involving stakeholders from all

identified critical infrastructure sectors, all states of the federation and from all levels of government and industry.

- ii. Provide a clear call to action, which will leverage on the coordination, cooperation, collaboration, and smart risk management procedures, and focus on specific actions germane to the policy goals.

## **7.5 The Critical Infrastructure Sectors:**

- i. Policy preparatory process on NCIIPP carried out a general national survey with the goal of identifying critical infrastructure sectors whose strategic operational backbone rely on functional and secure National Critical Information Infrastructure.
- ii. The policy identifies the following infrastructures.
  - a. Communications Sector
  - b. Government Facilities Sector
  - c. Manufacturing Sector
  - d. Dams Sector
  - e. Defence Sector
  - f. Chemical Sector {Oil and Gas}
  - g. Power and Energy Sector
  - h. Commercial Facilities Sector
  - i. Financial Services Sector
  - j. Food and Agriculture Sector
  - k. Emergency Services Sector
  - l. Transportation Systems Sector
  - m. Public Health and Healthcare Sector
  - n. Water & Waste Water systems
  - o. Information Technology Sector
- iii. Effective risk management requires an understanding of the significance of assets, systems, networks, as well as the associated dependency and interdependency of critical infrastructure.
- iv. Consequently, the policy encourages stakeholders to identify critical functions and resources that impact on their businesses and

communities in order to support preparedness, planning and capability development.

- v. The policy describes a national unified effort to achieve critical infrastructure security and resilience. Given the diverse authorities, roles, and responsibilities of critical infrastructure partners, a proactive and inclusive partnership among all levels of government and the private and non-profit sectors is required to provide optimal critical infrastructure security and resilience.

## **7.6 Coordination Policy Specific to NCIIPP**

- i. The NCIIPP for each sector details sector level performance objectives and feedback to the coordinating agency of government charged with the responsibility of managing the sector.
- ii. The NCCC shall be empowered through legislation to provide the following national critical information infrastructure protection roles:
  - National Coordination and Reporting Mechanism of cybersecurity incidents for critical infrastructure.
  - NCCC shall facilitate development and implementation of national criteria on best practices approach at each critical information infrastructure sector.
  - NCCC shall facilitate the development of a national Critical Information Infrastructure Measurable Program (CIIMP) as part of the cohesive National Cybersecurity Strategy.
  - NCCC shall assist government and the private sectors to mitigate their cyber-risks
  - It shall provide legal framework for investigating cyber security incidents.

- Promote regional and international cooperation on NCIIPP across national boundaries and assist in determining transnational solutions.

## **PART EIGHT**

### **PRINCIPLES ON ASSURANCE & MONITORING**

#### **8.1 Introduction:**

- i. Vulnerabilities exist in critical national information infrastructure for several reasons including: technological flaws, non-existent or weak security controls, non-compliance with defined security policies, dearth of effective mitigating strategies and plans amongst others.
- ii. Absence of a feedback reporting mechanism on how effective implemented controls are safeguarding the nation's cyberspace will lead to an assumed, unverified and false sense of protection.
- iii. The policy provides for the creation of a National Assurance & Monitoring mechanism for the nation's cyberspace.

#### **8.2 Focal Points:**

The National Assurance & Monitoring Mechanism, under the supervision and coordination of NCCC will achieve the following outcomes:

- i. Motivate compliance to national cybersecurity standards.
- ii. Ensure collection of relevant data that validates previous cyber security initiatives, and support its' on-going improvements.
- iii. Provide feedback on the status of the nations' cyber security posture, thus enabling stakeholders, partners and policy-makers to develop sound cyber security countermeasures and risk mitigation strategies.

- iv. Increase confidence that responsible stakeholders are complying with statutory cybersecurity requirements and frameworks
- v. Ensure efficient and effective solutions are deployed to protect the nation's cyberspace.
- vi. Ensure awareness of evolving threats to the nation's cyberspace thereby enabling proactive defence measures.

# PART NINE

## PRINCIPLES ON NATIONAL COMMITMENT & GOVERNANCE

### 9.1 Introduction:

- i. Nigeria is committed to establishing the highest level of governance and commitment in tackling cybercrime. To achieve this goal it will design and implement appropriate, sustainable and effective policies and practices. The ONSA will provide oversight responsibilities on matters relating to policies, practices, individuals and organizations charged with the responsibility of combating cybercrime.
- ii. The national commitment will ensure that these practices are continually being reviewed and improved by benchmarking against internationally accepted best practices and lessons learned.
- iii. The outcomes of the national commitment on governance are:
  - To give Nigerian citizens and the rest of the world comfort and understanding of our resolve and stance on tackling cybercrime.
  - Allow the nation to identify progress on the key strategies that need to be implemented
  - Steer the country towards efficient and transparent methods of conducting operations for cybercrime especially where there are conflicting objectives.
- iv. It is the policy of the Government of Nigeria to have and maintain principles on national commitments and governance.
- v. These principles will allow the nation to foster cooperation and coordination in the drive to maintain a positive image across local, regional and global communities in the nation's drive to reduce the effects of cybercrime.

## **9.2 Nature of Commitment**

- i. In order to ensure the fight against cybersecurity in Nigeria is sustained. Nigeria commits to putting in place perpetual counter-measure instruments and cybercrime fighting environment that will be sufficiently funded and which in turn will be monitored and supported by the national security agencies.
- ii. It will ensure that it appoints the most suitably trained and qualified individuals to oversee the delivery of its commitment to combat cybercrime and make it difficult for cybercriminals to successfully operate within the nation's cyberspace.

## **9.3 Nature of Governance**

- i. In order to ensure the fight against cybercrime is successful, the government will commit to putting in place, effective governance and control mechanisms to ensure its national security agencies have appropriate oversight of the activities within its cyberspace environment.
- ii. This will include amongst other areas identifying the institutions and bodies that control activities and services that can impact on its cyberspace environment. Such organizations and bodies will include but are not limited to;
  - Internet Service Providers
  - Domain Name Registration Body
  - Telecommunications Service Providers
  - Internet Exchanges; and
  - Other associated bodies
- iii. The governance oversight will allow for centralization, prompt and effective response to cybercrime activities.

## **9.4 National Legal Commitments**

- i. An integral part of the nation's National Cybersecurity Policy is the adoption of regional and international harmonized legislations against the misuse and abuse of cyberspace for criminal and other unlawful purposes.
- ii. In order for Nigeria to ensure its policy on cybercrime is successful, Nigeria commits to enacting appropriate laws relating to cybercrime.
- iii. The nation's commitment will include reviewing these laws on a regular basis so that they can be updated when the need arises. The benefit of this approach will be that the nation's legal landscape will be adaptable to the changing cybercrime environment.

## **9.5 Regional Commitments and Governance**

- i. To ensure its policy on cybercrime is comprehensively successful, Government commits to fostering initiatives for the cooperation, collaboration, information sharing and coordination of anti-cybercrime strategies with countries, law enforcement agencies and regulatory bodies in the African Region.
- ii. Government will build and foster partnerships with willing and participating countries by sharing information and combining efforts to combat cybercrime.
- iii. Nigeria will engage in regional discourse, consultations and negotiations that impact positively on regional cybersecurity efforts.

## **PART TEN**

### **PRINCIPLES ON ONLINE CHILD ABUSE & EXPLOITATION**

#### **10: 1 Introduction:**

- i. The Nigerian Cybersecurity Policy recognizes growing engagement of the nation's active young population in cyberspace.
- ii. The resultant impact of this engagement has contributed significantly to digital knowledge acquisitions and economic empowerment of this critical segment of the nation's population.
- iii. Unrestricted access to digital contents, contacts and communications through Cyberspace has raised new areas of national security concern on vulnerability, exploitation and abuse especially as it affects this critical segment of the nation's population.
- iv. There are growing national concerns on the distribution of digital content and materials targeted to young population which are making them vulnerable to cyber-terrorism recruitment, child pornography, sexual abuse, harassment, exploitation, extremism, violence and human trafficking resulting into unpleasant outcomes.

#### **10.2 Strategic Areas of Focus:**

- i. National Cybersecurity Policy will work within the current and future legislative frameworks to provide countermeasure mechanisms on Online Child Abuse and Exploitation within the nation's cyberspace.
- ii. The policy provides for a partnership framework for counter-measures towards safeguarding the safety and security of the Nigeria children online.

- iii. The policy seeks membership of relevant global law enforcement bodies, which provides a 24/7 mechanism to receive reports about illegal behavior or content from persons in member countries.
- iv. The policy seeks for national awareness and capacity building of Nigerian law enforcement community and the judicial sector on countermeasures, investigating child online abuse and exploitation as well as prosecution within current and future legislation.
- v. The policy seeks for the creation of national mechanisms guaranteeing that Child Abuse Materials found in the nation's cyberspace are channeled towards appropriate law enforcement apparatus within the Nigeria Police Force.
- vi. The policy seeks for the development of working mechanisms to provide means for reporting illegal content found in the country's cyberspace, which has the capacity to respond rapidly and have illegal materials removed or rendered inaccessible.
- vii. The policy seeks for multi-stakeholder partnership, bilateral and multilateral cooperation, collaboration and information exchanges on online crime against children.

## **PART ELEVEN**

### **MISCELLANEOUS PRINCIPLES**

- i. It is the policy of the Nigerian government to provide and sustain continuity of government in the advent of cybersecurity emergency.
- ii. The policy seeks citizen's proactive and collective participatory measures towards ensuring that national cybersecurity policy obligations are effectively respected in regards to national security, strategic economic interest and patriotism.