

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 21st 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.

NATIONAL CYBERSECURITY STRATEGY

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 National Cybersecurity Strategy as cohesive national measures towards addressing the challenges. These measures contain strategic initiatives and programs that are aligned with the national doctrines, principles, vision, goals and objectives as enshrined in the National Cybersecurity Policy. The strategy recognizes three key approaches to a successful national cybersecurity engagement: public private sector partnership; stakeholders' collaborations and international cooperation.

Our commitment is to ensure continuity of government in the advent of cyber threat emergency, safeguard critical information infrastructure, and nurture national cybersecurity readiness through the engagement of all stakeholders.

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 CONTENTS

FOREWORD BY NATIONAL SECURITY ADVISER.....

TABLE OF CONTENT.....

EXECUTIVE SUMMARY.....

Chapter One:

AN OVERVIEW OF NATIONAL CYBERSECURITY STRATEGY

1.1. Introduction.....

1.2. National Cybersecurity Vision.....

1.3. The Aim of National Cybersecurity Strategy.....

1.4. Cyberspace Within the Context of National Prosperity & Opportunities.....

1.5. Cyber-Risk within the Context of National Security & Economic Impact

1.6. Cybersecurity within the context of National Security Strategy.....

Chapter Two:

UNDERSTANDING NATIONAL CYBER-RISK EXPOSURE

2.1 Introduction.....

2.2 Cyber-threat Landscape & Impacts.....

2.3 Imperative of a National Vulnerability Assessment.....

2.4 Gauging Impacts and Opportunities.....

Chapter Three:

NATIONAL READINESS STRATEGY

3.1 National Cybersecurity Policy Direction.....

3.2. Necessity of a National Cybersecurity Strategy.....

3.3. Objectives of National Cybersecurity Strategy.....

3.4 Scope of National Cybersecurity Strategy.....

3.5 Approach, Guiding Principles, & National Priorities.....

3.6 Governance Strategy.....

Chapter Four:

LEGAL FRAMEWORK INITIATIVES

4.1 Objectives.....

4.2 Approach.....

4.3 Initiatives.....

4.4 Special Areas of Focus

Chapter Five:

NATIONAL INCIDENT MANAGEMENT STRATEGY

5.1 Purpose.....
5.2 Establishing National CERT.....
5.3 Implementation Approach.....
5.4 Preventive Strategy.....
5.5 Detection Strategy.....
5.6 Response Strategy.....
5.7 Cooperation and Partnership.....
5.8 Capacity Building.....
5.9 National Digital Forensic Mechanism.....

Chapter Six:

STRATEGY ON CRITICAL INFORMATION INFRASTRUCTURES PROTECTION

6.1 Introduction.....
6.2 Vision of CIIPR.....
6.3 Mission of CIIPR.....
6.4 Strategic Objectives.....
6.5 Strategic Imperatives to Achieve Aims and Objectives.....
6.6 Initiative 1.....
6.7 Initiative 2.....
6.8 Initiative 3.....
6.9 Initiative 4.....
6.10 Success Criteria and Review of CIIP Strategy.....

Chapter Seven:

STRATEGY ON ASSURANCE & MONITORING

7.1 Introduction.....
7.2 Strategic Objective.....
7.3 The Cybersecurity Assurance Context.....
7.4 Focal Points.....
7.5 Strategy.....

Chapter Eight:

NATIONAL CYBERSECURITY SKILL & MANPOWER DEVELOPMENT

8.1 Introduction.....
8.2 Objectives.....
8.3 Scope.....
8.4 Initiatives.....
8.5 Roadmap for Nigeria Cybersecurity Industry.....
8.6 Institutional Framework.....

Chapter Nine:

STRATEGY ON ONLINE CHILD ABUSE & EXPLOITATIONS

9:1 Introduction.....
9.2 Rationale for COAEP.....
9.3 Objectives.....
9.4 Strategic Approach.....
9.5 Strategy
9.6 Operational Measures.....
9.7 National Security Response Measures.....

Chapter Ten:

STRATEGY ON PUBLIC-PRIVATE PARTNERSHIP

10.1 Introduction.....
10.2 The Imperative of PPP framework for NCSS.....
10.3 Public-Private Sector Partnership Management Strategy.....

Chapter Eleven:

STRATEGY ON NATIONAL INTERNET SAFETY

11.1 Introduction.....
11.2 National Internet Safety Initiative.....
11.3 Objective.....
11.4 Scope.....
11.5 Initiative.....
11.6 Importance Of Nisi to NCCC.....

FIGURES

- Figure 1:** Sources of Cyber-threat
- Figure 2;** Initiatives Pyramid
- Figure 3:** Data Protection and Privacy
- Figure 4:** Data Protection Impact Point
- Figure 5:** Four Pillars of Critical Infrastructure Protection [adapted from ITU's A Generic National Framework for Critical Information Infrastructure Protection (CIIP)]
- Figure 6:** The Cybersecurity Assurance context -It shows the logical environment within which the Cybersecurity Assurance mechanism will operate and monitor.
- Figure 7:** The proposed linear build-up process coordination through Special Purpose Vehicle

EXECUTIVE SUMMARY

The economy of a modern Nigeria is anchored and sustained on two major infrastructural landscape (i.e. Physical and Digital) working together to sustain critical and non-critical sectors of the economy in Government, Manufacturing, Dams, Defence, Chemical Sector {Oil and Gas}, Power and Energy, Commercial Facilities, Financial Services, Food and Agro-allied, Emergency Services Transportation Systems, Public Health and Healthcare Sector, Water and Waste Water systems. Digital infrastructure is the National Information Infrastructure (NII) component that permeates the physical infrastructural landscape supporting it to function seamlessly, endlessly and sustainably. The NII is the backbone of the nation's active presence in cyberspace. Significant disruption of its operation will undermine the confidentiality, integrity and availability of essential national services, which will be inimical to national economy and security.

In comparison with other industrial and commercial entities, the Internet has been with us for a relatively short period of time. It has been responsible for the most revolutionary and rapid changes to the way we communicate, undertake business, perform job functions as well as boost our military strategies. We have seen the examples in the home schooling, social media and cloud computing rising on the tails of the Internet phenomenon.

The Internet has given the phrase "global village" an appropriate meaning, this is driven home with the illustration that an individual in Nigeria can immediately set up an online conference call and chat with group of people on the other side of the planet in real-time. The majority of users of the Internet conduct their activities in a legitimate and above board manner, while on the other side of the internet there are individuals, organisations, foreign intelligence agencies and state sponsored actors that have used the very benefits of the internet, i.e. its speed, global presence and openness, to carry out criminal activities that can cause havoc to those that are not aware, prepared or equipped to deal with such undertakings.

This document therefore examines the strategic imperative of a national cybersecurity. It highlights various strategies that will be used to implement the measures outlined in the new National Cybersecurity Policy.

These include the following:

- The development and implementation of appropriate legal framework, with initiatives that will allow for the identification and prosecution of cybercrimes that impact Nigeria regardless of whether they originate within Nigeria or are launched from outside of the country. It encompasses training the judiciary, security and law enforcement agencies, seeking international co-operation, public and private sector co-operation and public awareness programmes. It also introduces a special focus on data protection, privacy and lawful interception.
- Establishment of a National Incidents Management Strategy which outlines the commissioning of a National Computer Emergency Response Team (CERT) and introduces the roadmap for implementing Detective, Preventative and Response capabilities to deal with cybercrime activities.
- The strategy for Protecting Critical information Infrastructures including shared responsibility between government and owner operators of critical infrastructure. It also highlights the ways in which early warning, detection, reaction and crisis management will be assessed, developed and implemented to provide a proactive readiness to react to and deal with threats towards Nigeria's Critical Infrastructures.
- The strategy seeks to ensure the development of information security assurance and monitoring plan. It includes a new national mechanism on cybersecurity assurance, adoption of fit for purpose standards for Governance, Risk and Control, Core Assurance Capabilities, National Enterprise Architecture Framework. It also endorses the adoption of application security testing as well as the adoption of a Balanced Scorecard Framework for cybersecurity.
- The introduction of a sustainable strategy to develop, maintain and ensure Nigerians are informed and equipped to deal with cybersecurity events by establishing a mechanism for Cybersecurity Skill and Manpower Development initiatives. These initiatives will be driven through public-private partnership. It introduces a model for certification of individuals to ensure quality of competence in the field of cybersecurity relevant to the nation.

- The strategy for protecting Nigerian Children from Online Child Exploitation and Sexual Abuse includes initiatives, such as the national awareness programmes through multi-stakeholder engagement, and international cooperation in the countermeasures.
- The Strategy on Public-Private Partnership highlights the need for interagency collaboration with private sector. It engages the framework for a public and private partnership in developing a cohesive response to mitigating cyber-risk.

In conclusion, The National Internet Safety initiative is aimed at providing general public awareness, education, and advocacy through multi-stakeholders' engagement, development of local tools, training software and applications in Internet safety and security readiness. It provides mechanism for gauging the nation's cyber security posture.

December 2014.

CHAPTER ONE

AN OVERVIEW OF NATIONAL CYBERSECURITY STRATEGY

1.1 Introduction:

1.1.1 National Cybersecurity Strategy (NCSS) is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community.

1.1.2 The NCSS comprises of short, medium and long term mitigation strategies covering all national priorities, addressing the nation's cyber risk exposure. Specific key cyber threats worldwide inimical to National interest are identified. Such as;

- i. Cybercrime
- ii. Cyber-terrorism
- iii. Cyber conflict
- iv. Cyber espionage
- v. Child online abuse and exploitation.

1.1.3 These threats have significant capability to damage the integrity of the nation, disruption of critical information infrastructure operations, undermine government operations and national security.

1.1.4 The NCSS articulates, coordinates and guides the country in the implementation of National Cybersecurity Policy and cohesive counter-threat measures for the protection, security and defence of National Cyberspace.

1.1.5 The Strategy provides various initiatives for the focused areas and national mechanisms for developing and implementing Legal & Policy Measures, National Incident Management, Critical Information Infrastructure Protection, Cybersecurity Assurance Framework, Manpower Development, Child Online

Abuse & Exploitation, National Internet Safety, Public Awareness, Multi-Stakeholder Partnership and Global Cooperation on Cybersecurity.

1.2. National Cybersecurity Vision:

The National Cybersecurity Policy has set out a clear purpose, direction and outcome of the country's engagement in cybersecurity.

What is the Nigeria Cybersecurity Vision?

A safe, secured, vibrant, resilient and trusted community that provide opportunities for its citizenry, safeguard national assets and interests, promote peaceful interactions and proactive engagement in cyberspace for national prosperity – Culled from National Cybersecurity Policy 2014

1.3. The Aim of National Cybersecurity Strategy:

The aim of the NCSS is to provide a cohesive roadmap, initiatives, and implementation mechanism for achieving the national vision on cybersecurity.

1.4 Cyberspace Within the Context of National Prosperity & Opportunities:

1.4.1 Cyberspace offers excellent platforms and opportunities for securing and growing the nation's economy.

1.4.2 Every citizen that is connected to cyberspace through the internet is immeasurably impacted and empowered for actions.

1.4.3 In the next few years, Nigeria will become a broadband economy where every individual and corporate citizens will have unhindered wholesome access to the internet.

1.4.4 Cyberspace will become the mainstream for national integration and digital economy empowerment. It is a knowledge driven space with massive capacity to bridge gaps in mobility, commerce, innovations, education, poverty reduction, and economic empowerment.

1.4.5 What is the Cyberspace?

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. – Culled from National Cybersecurity Policy 2014

1.4.6 Why is Cyberspace important to the National Government?

It has been established that we have the contemporary four (4) domains of land, Sea, Air and Space, Nigeria recognizes Cyberspace as the fifth (5th) domain for driving critical national functions such as economic development, commerce and transactions, social interactions, medical and health, government operations, national security and defense.

1.5 Impact of Cyber-Risk on National security and the Economy

1.5.1 The nation's digital economic existence relies on the effective functioning of digital infrastructure. In Cyberspace, the country is not isolated but interconnected to other countries and active actors within cyberspace through interdependent networks of information infrastructures. Thus, the country is exposed to predictable and unpredictable risks.

1.5.2 Just as we have actors with legitimate intentions so also exist other actors with illegitimate and malicious intentions. Within the global network of networks there are critical structural flaws which can be exploited for criminal intents and purposes against the country to compromise the confidentiality, integrity, availability and accessibility of the nation information systems and critical information infrastructure.

1.5.3 Vulnerabilities exist within cyberspace that can be used to exploit national economic interest and constitute threats to National Security. For instance, recent compromise of some government websites, growing underground cybercrime industry, emergence of activism through online backdoors, fraudulent practices, incidence of online exploitation of the young segment of the population, gross abuse of the social media for waging malicious campaign against the state, conflict and violence perpetuated through internet, economic sabotage through distributive denial of critical services, coordinated cyber espionage, malicious intrusion into computer systems and other digital devices, cyber piracy and stealing of intellectual assets, cyber-terrorism, online financial crime and money laundering, distribution of offensive contents and child abuse materials and hosts of other malignant activities committed through cyberspace are all inimical to the wellbeing of the country. The economic impact is destructive to any nation.

1.6 Cybersecurity within the context of National Security Strategy:

Providing security for the critical information infrastructure and other critical components of information system within the current state of affairs is a huge national challenge.

National Security needs the infusion of a cohesive framework on cybersecurity to provide holistic approach to the current and future security landscape, because the nation security and economic terrain is fast paced and is moving towards a digitally enabled and mobile terrain.

State and non-state actors involved in cyber-crimes are adequately equipped with sophisticated cyber tools to cause damage with unprecedented dimension.

The security inclusion of cyberspace domain will help the country prepare and response to such security threat and help address the country's weakness in her own digital vulnerability, as well as strengthening our ability to provide countermeasures in partnership with other legitimate state and non-state actors. This is the strategic rationale for the development of National Cybersecurity Policy and the context within which National Cybersecurity Strategy is articulated for national security readiness.

CHAPTER TWO

UNDERSTANDING NATIONAL CYBER-RISK EXPOSURE

2.1 Introduction

In line with the national doctrine on cyber-risk exposure as reflected in the National Cybersecurity Policy document, the country presence in cyberspace exposes it to a new dimension of risk. Therefore, development of the country's Cybersecurity Strategy is approached from examining security risk exposure of the whole country.

What Is Cyber-risk?

Cyber risk is the possibility that a threat and vulnerability exists within the nation's cyberspace inimical to the security and safety of information systems and associated infrastructures. Furthermore, it is the possibility that the threat will exploit a vulnerability to breach the safety and security of an information system and or information networks or infrastructure.

National cyber-risk has two (2) major components:

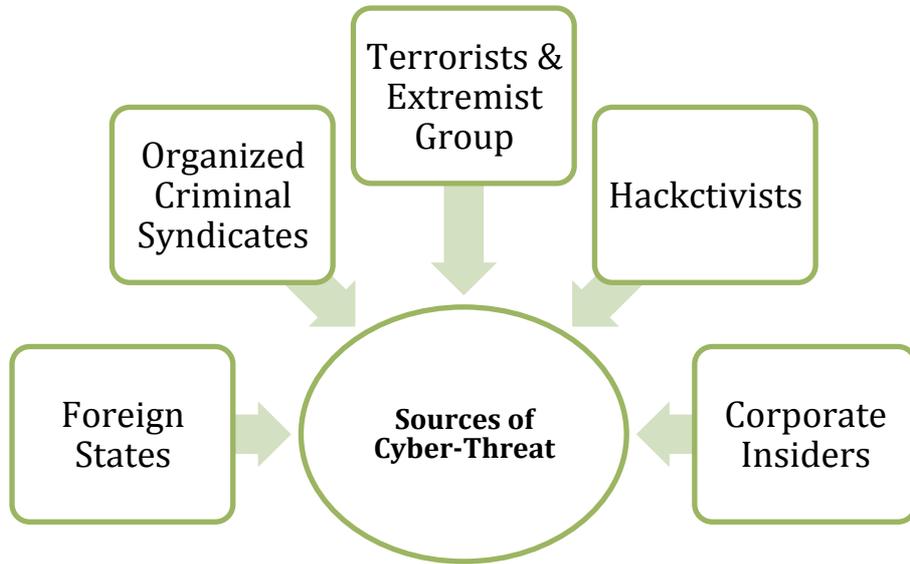
- i. Cyber-threat
- ii. Vulnerability

2.2 Cyber-threat Landscape & Impacts:

2.2.1 Cyber threat is the possibility of a malicious attempt to damage or disrupt the operations of a vulnerable computer network and information system.

2.2.2 The nature and the dimension of the impact of cyber-threat are diverse and it involves a **threat actor** who performs a pre-mediated attack or exploit circumstances of an accident. A threat actor is engaged by a **threat source** either clandestinely or tactically. A threat source initiates a desire to breach access to critical information or security controls with the purpose of benefiting from the breach, for example for financial gain or competitive advantage in the case of industry cyber espionage.

Sources of Cyber-threat



NCSS Fig. 1

2.2.3 **Cyber threat** is escalated to **cyber-attack** by a **threat actor** where a deliberate effort is initiated to exploit the vulnerability of computer systems, information and communication networks, and internet driven processes for criminal intent and malicious purpose.

2.2.4 It usually involves the use of malicious codes to alter digital codes, logic or data, resulting in disruptive consequences that can compromise the confidentiality, integrity, and availability of data and lead to manipulation of information systems and internet network infrastructure.

2.2.5 Cyber-attacks may lead to the following consequences: Identity theft, fraud, extortion, Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses, manipulation of hardware, denial-of-service and distributed denial-of-service attacks, breach of access, password sniffing, system infiltration, website defacement, private and public web browser exploits, instant messaging and social media abuse, and intellectual property theft.

2.2.6 Economic Impact of Cybercrime

- Recently, a total of \$388 billion USD was estimated as the approximate total financial loss to cybercrime in more than 24 countries in the last six years.
- The global black market in marijuana, cocaine and heroin combined (\$288bn) and approaching the value of all global drug trafficking (\$411bn).
- At \$388bn, cybercrime is more than 100 times the annual expenditure of UNICEF (\$3.65 billion).¹
- Physical crime are becoming digital. More criminals that were involved in traditional crimes are moving towards the Internet. They know that it's easier, more profitable and the probability of being caught is lower

- Nigerian financial consumer loss to Cybercrime in 2010 stood at N2,146,666,345,014.75 (\$13,547,910,034.80) to cybercrime in 2012²

-

2.2.7 Cyber threat landscape is diverse and diffusely driven by state and non-state actors.

State Actor:

The State Actors are established and well organised to carry out the most sophisticated threat in the cyberspace with the goal of exploiting computers and information and communication networks to gather intelligence on government, military, industrial and economic targets, and opponents of their Regimes. They gathered intelligence data and information which can be used for spreading falsehood and disrupting critical services. Sometimes they install hidden malicious software on a system can be adapted to suit an attacker's changing objectives, lying hidden within the system in readiness for exploitation during times of increased tension or conflict.

Non State Actors:

Organized and unorganized criminals operating in the underground economy exploiting weakness in individual, corporate and government systems and information infrastructure. They used different technology and psychology method to manipulate users and engage highly sophisticated cyber tools to infect, hijack, control and extract value information for criminal purpose. Financial motivation is usually the driven force of this particular non-state actor. They inflict huge financial damage on their victims. Their action damage country reputation and inflict huge collateral damage on the country financial system.

Terrorists and extremist engage resources of cyberspace to perpetuate against the government; falsehood, communication, recruitment, indoctrination, raising of fund activists and distribution of extremist contents. They are active attackers and constitute one of the major threat to national security.

² *Economic Cost of Cyber Crime in Nigeria* by Gbenga Sesan, Babatope Soremi and Bankole Oluwafemi as part of the output for the Cyber Stewards Network Project of The Citizen Lab, Munik School of Global Affairs. University of Toronto and Supported by international development research centre.(IDRC)

Activist with unwholesome pattern of obtaining information used against established authorities. They operate through social media and vulnerable backdoors, usually connecting with an insider with passive attack tendency.

2.2.8 The National Cybersecurity Policy document has identified and classified five (5) major cyber threats as inimical to the national security strategy. These threats have significant capability to cause considerable damage to the integrity of the country's economy.

2.2.9 The underlying ideology of this National Cybersecurity Strategy is to proffer relevant strategic frameworks and mechanisms for addressing these cyber-threats, securing the nation in the advent of cyber-attack, while preparing the nation for a proactive engagement towards building and nurturing a safe and secure cyberspace where trust and confidence are hallmark of Nigeria cyber-community.

2.3 Imperative of a National Vulnerability Assessment

2.3.1 Vulnerability is the structural weaknesses of the nation's information systems and critical information infrastructure ranging from technical flaws, porous measures, to human negligence.

2.3.2 The NCSS requires that national vulnerability assessment be conducted towards determining weaknesses in government information systems, websites, networks, data handling processes and vulnerabilities existing in the nation's critical information infrastructure.

2.3.3 The national vulnerability assessment helps the government appreciate the level of her unpreparedness, the need to safeguard huge investments in information systems and communication infrastructure and commitment made to global partners National ICT developmental goals.

2.3.4 There are efforts aimed at addressing some of these challenges at the sectorial levels. However, NCSS is laying a foundation for the coordination of the country cyber-ecosystem with a unified framework on cybersecurity.

2.3.5 The ultimate goal is to build a collective counter-measures mechanisms that will facilitate the country's capability in addressing the huge vulnerability gaps among the states information systems, critical information infrastructure, and protection of our presence in cyberspace.

2.4 Gauging the Impacts and Opportunities

2.4.1 There are many advantages associated with the implementation of the national Cybersecurity strategy. Building and nurturing trust and confidence in the use of national information systems and critical information and communication technology is crucial to the socio-economic well-being of the citizenry, therefore it is important to secure our nation in cyberspace thereby infusing high level of confidence and trust in the nation digital economy.

2.4.2 The nation depends on the functioning of information and communication technology and the operation of critical information infrastructures. Our interactions, transportation, communication, trading and e-commerce, financial services, mission critical services are relying on the confidentiality, integrity and availability of information flowing through these infrastructures.

2.4.3 National enterprise security architecture is further enhanced with the inclusion of cybersecurity strategy. A new and holistic National Security Architecture will emerge by integrating physical and cyber security as countermeasures against external threat, thus consolidate the country readiness capability.

2.4.4 The country's emerging opportunities as a result of her trusted presence in cyberspace are inclusive of the following;

- A resilient digital economy, stimulating innovations, wholesome engagement, development and inflow of foreign direct investment.
- An opportunity to exploit cyberspace to advance the country's military capability in engaging external threat, conflict, violence and terrorism.

- Nigeria's readiness to defend her citizens, safeguarding operations of critical information infrastructures and extra-territorial jurisdiction in time of unpredictable cyber-attack, ensures continuity of critical operations amidst adversaries.

CHAPTER THREE

NATIONAL READINESS STRATEGY

3.1 National Cybersecurity Policy Direction

3.1.1 The National Cybersecurity Strategy defines the nation's readiness to safeguard and prepare the whole Nation in advance for global economic competitiveness in cyberspace. It also addresses willingness to empower the nation in building a comprehensive, coherent, structural and procedural capabilities at strategic and tactical levels in mitigating cyber risks.

3.1.2 The strategy involves engagement of government and non-government actors, employing multi-stakeholder's principles of approach, inclusive of all participatory and partnerships of government, industry and other stakeholders.

3.1.3 The critical success factor of NCSS is hinged on comprehensive mobilization, engagement and coordination of critical components towards securing our presence in cyberspace and protecting critical information infrastructures.

3.1.4 The direction of the policy of government on cybersecurity is in agreement with regional and global direction on securing cyberspace.

3.1.5 The paramount focus of the cybersecurity strategy is addressing our cyber risk exposure, protection of our national critical information infrastructure, exploiting cyberspace opportunities for national security and economic goals, and the enthronement of a trusted cyber community remain a paramount focus of the National Cybersecurity Strategy.

3.2 Necessity of a National Cybersecurity Strategy

3.2.1 The multi-dimensional nature of the evolving security threats is moving the current National Security Strategy beyond the traditional scope.

3.2.2 The nature of the current security threats such as cybercrime, violence, conflict and terrorism increasingly exploits the openness and borderless nature of cyberspace. This constitutes a threat to our growing dependence on cyberspace.

3.2.3 Government is leading a coherent national response towards reducing the impact and escalation of cyber threats in a manner that safeguards the nation's presence and guarantee trust and confidence in our connected economy.

3.3. **Objectives of National Cybersecurity Strategy**

3.3.1 The Strategy aims are to set out a national roadmap with various coordinated mechanisms; harness implementation framework; and actions that will guarantee attainment of the National vision, mission and goals on Cybersecurity as captured in the National Cybersecurity Policy.

3.3.2 Therefore, the Strategy is needed to achieve the following specific objectives:

- i. A comprehensive cybercrime legislation and cyber-threat counter measures that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace.
- ii. Provision of measures that protect critical information infrastructure, as well as reducing our national vulnerabilities through cybersecurity assurance framework.
- iii. To articulate an effective computer emergency response capability.
- iv. National mechanisms on capacity building, public awareness, skills empowerment is necessary to help strengthen our capability so as to respond promptly and effectively to cyber-attacks.

- v. A trusted mechanism for engaging national multi-stakeholder and international partners towards collectively addressing cyber threats.
- vi. To deter and protect government from all forms of cyber-attacks.
- vii. To coordinate cybersecurity initiatives at all levels of government in the country.
- viii. To build national capabilities against cyber threats with coherent cooperation through public- private sector partnership and multi-stakeholder engagement.
- ix. To promote national vision on cybersecurity through awareness, partnership through shared responsibilities and a trusted community of stakeholders.
- x. To promote coordination, cooperation and collaboration of regional and global stakeholders on cybersecurity.

3.3.2 The Strategy is further aligned with National Security Strategy and other relevant government documents most especially National ICT policy and National broadband plan.

3.3.3 The Strategy defines the basis for a coordinated national and globally compatible framework for action, cooperation and approach to protecting national critical information infrastructure against cyber threats.

3.4 Scope of National Cybersecurity Strategy

The scope of the national cybersecurity strategy covers the areas of national priorities as well as general framework for partnership and international multi-stakeholder cooperation on cybersecurity.

3.5 Approach, Guiding Principles & National Priorities

The NCSS approach involves coordination of the nation's cybersecurity constituents and public-private partnership which are consistent with the objectives and the guiding principles as encapsulated in the National Cybersecurity Policy.

3.6 Governance Strategy

3.6.1 The implementation of the provision of the strategy will be coordinated through the Office of National Security Adviser in collaboration with other relevant government agencies.

- 3.6.2 The central coordination model will operate in synergy with federated structures toward achieving comprehensive measures on cybersecurity.
- 3.6.3 Central coordination model is adopted in line with international best practices and has recommended in the global framework for cooperation on cybersecurity
- 3.6.4 The sustainability and critical success factor of this governance model is anchored on public-private sector partnership, multi-stakeholder engagement as well as regional and international cooperation.

CHAPTER FOUR

LEGAL FRAMEWORK INITIATIVES

4.1 Objective

4.1.1 The objective of the Cyber Security Legal Framework is to identify the strategy required to ensure areas defined in the Cyber security Policy are implemented, managed, sustained and effective in combating cybercrime in Nigeria.

4.1.2 To achieve this aim, a number of immediate and long term legal framework initiatives will need to be developed, agreed, funded and rolled out to accomplish success.

4.2 Approach

- The approach takes the form of referencing aspects of the Legal Framework in the cyber security policy with a view to prescribing the initiatives that will allow for the implementation of each of the detailed areas.



NCSS Fig 2 Initiatives Pyramid

4.3 Initiatives:

4.3.1 Initiative 1: Enacting Fit for Purpose Cybercrime Legislation

- As prescribed in the cyber security policy, fit for purpose legislation will need to be enacted and implemented to combat cybercrime.
- The main focus of this initiative will entail a root and branch review of Nigeria's current and draft cybercrime legislations.
- The objective of this exercise will be to identify any gaps between what is currently available and what has been proposed in the Cyber security policy with a view to updating any omissions or redundancies so that when the legislation is enacted, it will be adequately effective, workable and flexible enough to deter and prosecute cybercrime activities
- This initiative supports a strategy to enact a number of separate and distinct legislations that will make up the cybercrime legislative framework as opposed to a single legislation that has the banner of cybercrime legislation.
- To the barest minimum, the following legislations will need to be included in the new cybercrime framework: 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, Hacktivism; Identity Theft, Information Security, Intellectual Property Rights, Lawful Interception, Online Fraud, Privacy, tribalism and Xenophobia, Software Piracy, Security Breach Notifications, Unauthorized System Interference etc.
- Aligned to the review and enactment of the cybercrime legislative framework is the need to put in place measures to keep the laws up to date and effective.
- The strategy to achieve this will include the establishment of a Cyber Crime Legislative Review Committee (CCLRC) whose purview will be to advise the National Security Advisor, Legislature and regulatory bodies on aspects of legislations that needs to be amended to ensure current legislations do not become redundant, unenforceable and ineffective.

- This is an immediate initiative and needs to be given special priority as it forms the bedrock of the applicability, enforceability and prosecution of individuals and organisations that breach key segments of the National Cyber Security policy.

4.3.2 Initiative 2.

Preparing and Revamping the Judiciary for Cybercrime Legislations

- Nigeria's current judicial environment is not adequately equipped to handle sophisticated cybercrime cases. In order to ensure the new cybercrime legislations are effective in the prosecution of alleged cybercrimes, when they are brought before the courts, it is the strategic objective of NCSS to ensure the Nigerian Court system is equipped to handle cybercrime cases.
- In fulfilling this strategy, the following initiatives will be undertaken
 - a) Capacity building for Judges and lawyers on the new cybercrime laws
 - b) Courts will be equipped to handle digital forensic evidence
 - c) Provide law enforcement agencies with the processes and procedures for investigating cybercrime activities.
 - d) Capacity building for law enforcement and security agencies on digital forensic capability.
- This will be achieved by developing a home grown fit for purpose certified programme of training courses, capacity building, awareness programmes and materials for current Nigerian judges and lawyers.
- The strategy will also include the inclusion of new cybercrime legislation courses in institutes of higher learning so that newly qualified lawyers have a basic understanding of Nigeria's cybercrime framework.
- This will be a long term and on-going initiative.

4.3.3 Initiative 3: International Co-operation

- To ensure our cybercrime laws are effective and internationally harmonised, the legal strategy is to adopt the provisions of the convention on cybercrime to enable effective cross border law enforcement.

- This will allow for the following:
 - I. International harmonisation of our legislations
 - II. Collation of all existing conventions and bilateral agreements
 - III. International cooperation to combat cybercrime
 - IV. wider investigatory capability
 - V. Capacity Building and knowledge sharing
 - VI. Opportunity for Nigeria to make a contribution to how cyberspace is governed through international instruments of law.

International co-operation will also include becoming a member of recognised bodies such as:

- The International Telecommunications Union (ITU)
- Cybercrime Convention
- Interpol

It is envisaged that the processes to engage with international bodies will start to be defined with the objective of implementing and achieving within the next 12 months.

This is an immediate initiative

4.3.4 Initiative 4: Public/Private Sector Collaboration

- Recognizing that cybercrime can impact both private and public sector environments, the legal strategy is to adopt processes for both public and private sector collaboration in combating cybercrime.
- As an example relationships between Communication Service Providers in assisting law enforcement agencies in preserving communications data for specified periods as dictated by the Data Retention legislations will be encouraged and forged.
- This will also extend to financial institutions in ensuring they retain customer records according to specified time lines.
- The strategy will also entail providing specific guidelines on how to meet these requirements.

- A key part of the public/private sector collaborative strategy will be to put in place measures to reduce reliance on foreign controlled networks to store personal information of Nigeria Citizens.
- This will have the impact of reducing the risk footprint as well as the potential for such data to be compromised and used to the detriment of Nigerians
- This is an immediate and ongoing initiative

4.3.5 Initiative 5: Raising Awareness

- While implementing cybercrime legislations are paramount in combating cybercrime, it is to be noted that making citizens aware of the threats and vulnerabilities that can accrue to them when they use the internet, is a measure that can be used to reduce the likelihood of them being victims of cybercrime.
- Raising awareness of the new laws through high profile campaigns is an initiative that will be used to make criminals aware of the consequences of being in breach of these legislations once they are enacted.
- It is also part of the strategy to socialise these new laws to the wider international community.
- This is an immediate initiative

4.4 Special Areas of Focus:

4.4.1 Data Protection, Privacy and Lawful Interception.

- Personal Information has economic and political value. The recent identification of Nigeria as a MINT (i.e. Malaysia, Indonesia, Nigeria and Turkey) country not only raises its profile in monetary and economic terms, it also raises the risk of infrastructure and systems containing Nigerian citizens data being targeted by unscrupulous individuals, organisations and nation states, leading to data loss, leakage as well as confidentiality, integrity and availability compromise.
- The recent revelations of American whistle-blower Edward Snowden has significantly raised awareness of the need for nations to put in place appropriate measures to protect the personal information, and privacy of its citizens.

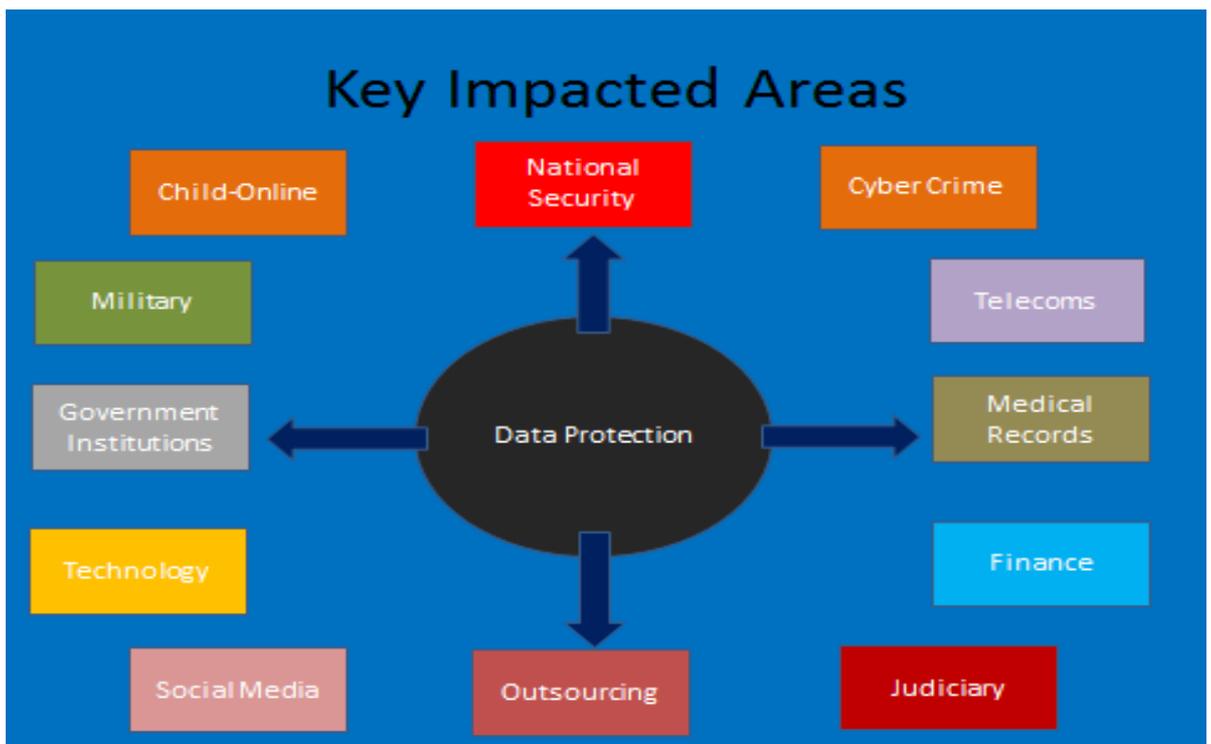
- The revelations also identified the need to protect and secure communications of not only high ranking government and high profile individuals from mobile phone tapping but also ordinary individuals from their everyday non-criminal conversations being intercepted and analysed by law enforcement agencies, organisations and foreign countries.
- To protect and legislate for criminal activities against Nigerian Citizens data and their communications special emphasis will be given to the development and roll out of Data Protection and Privacy laws in Nigeria.

NCSS Fig 3 Data Protection and Privacy

- The objective of this initiative will be to ensure individuals and organisations are aware of their responsibilities when handling and processing personal information.
- It will also allow them to be aware of what constitutes unacceptable and illegal behaviour in relation to the use of such information and communication streams.
- The legislative, technical and policy initiatives to fulfil this aim will consist of the following:

- i. Developing and enacting fit for purpose Data Protection and Privacy laws.
- ii. Defining minimum policy and standards requirements for handling personal information
- iii. Defining data Protection requirements for outsourcing initiatives.
- iv. Deploying an effective and transparent Lawful Interception regime.
- v. Deploying appropriate and workable data retention periods to assist law enforcement agencies in their investigations.
- vi. Defining Data Protection Requirements for safeguarding Nigerian Citizens details on government systems
- vii. Defining minimum technical measures that need to be in place to safeguard against personal information compromise
- viii. Identifying where Nigerian Citizens Data details are held and if systems held on are appropriately protected
- ix. Identifying Data Leakage Areas with view to reducing risk
- x. Developing and implementing fit for purpose guidelines
- xi. Liaison with Communication service providers to provide their customers with advice on how to protect themselves from cybercriminal activities
- xii. Liaison with both private and public sector commercial organisations to help them understand the measures they need to take to reduce their risks to data protection and privacy breaches

- xiii. Liaising with NCC , NITDA, Central Bank , Judiciary and Military to drive data protection in Telecoms, Finance and, government institutions and Judiciary
- xiv. Establishment of a new regulatory body for adjudicating and providing guidelines on Data Protection, Privacy and Lawful Interception
- xv. Reduce reliance on foreign-hosted cloud services for storing personal data of Nigerian Citizens.
- xvi. Long-term strategy is to Partner with Nigerian Service providers to develop capabilities to provide local cloud service capabilities.



NCSS Fig 4: Data Protection Impact Point

CHAPTER FIVE

NATIONAL INCIDENT MANAGEMENT STRATEGY

5.1 Purpose:

5.1.1 The strategy on incident management is designed to effectively deter and respond to cyber threats and cybercrime that will leverage on an efficient emergency readiness and coordination capability.

5.1.2 The strategy will also facilitate, promote and strengthen national commitments to regional and global partnerships and cooperation on cybersecurity.

5.2 Establishing National CERT:

5.2.1 The Nigerian Computer Emergency Team (ngCERT) shall be established to ensure efficient response to security incidents within our cyberspace.

5.2.2 An effective computer emergency response capability is essential to monitor and deter threats that can exploit information system vulnerabilities.

5.2.3 The Nigerian Computer Emergency Readiness Team (ngCERT) will be empowered by a legal framework through which its functions and responsibilities are defined.

5.2.4 However, where existing laws are inadequate, a review or new legislative processes should commence to address legal vacuum that will hinder operations of the national CERT.

5.2.5 The harmonized laws should clearly mandate it to function as one of the strategic components of the central coordinating center for all computer security incident management within our national cyberspace. Additionally, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.2.6 Additionally, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.3 Implementation Approach

5.3.1 A National Incident Response Plan (NIRP) will be formulated to achieve a coordinated emergency response protocols. It will govern both the national and sectorial CERTs

5.3.2 The plan will set out clear definitions and procedures for incident response that will focus on incident classification and its severance.

5.3.3 In addition, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.3.4 CEMS will classify threats that constitute a national-level cyber incident requiring ngCERT involvement and the triggering of incident response protocols.

5.4 Initiative 1: Preventive Strategy

5.4.1 All key national information infrastructures shall have a preventive mechanism for network monitoring system integrated into CEMS.

5.4.2 The preventive strategy will primarily be implemented by CEMS for analysis and detection as well as alert notification.

5.4.3 CEMS operational procedure will define the baseline security monitoring for broad detection of malicious or anomalous network activity within our cyberspace and specify specialized security monitoring for critical assets and critical processes within the context of the National Critical Information Infrastructure Protection Plan (NCIIPP).

5.5 Initiative 2: Detection Strategy

5.5.1 The Cyber Emergency Monitoring System (CEMS) will serve as the main provider of data analysis and reporting to other key detection and response partners across the incident management ecosystem.

5.5.2 Its key focus is to consistently monitor indicators within the nation's cyber space in order to detect potential threats and classify them according to its severance level determined. This can serve as an alert to trigger the next chain of activity in the response protocols.

5.6 Initiative 3 Response Strategy:

5.6.1 After an incident is detected and validated by the CEMS, direct and coordinated action will be implemented immediately to ensure that appropriate actions to stop an on-going incident occur at the right time on the right cybersecurity priorities.

5.6.2 The action plan will require identifying the scope and scale of the incident in order to activate the relevant countermeasures procedures as outlined in NIRP to mitigate damages.

Investigating cybercrime incident requires a strict evidence preservation procedures showing appropriate evidence handling procedure and

established chain of custody.

Therefore, it is necessary for incident handlers to take appropriated measures in order to preserve any artefacts that could be of evidential value by recording, reviewing and resolving security incidents with the established incident management processes as define in the NIRP. Additionally, ngCERT is expected to document all such report as will be required to be submitted by all monitored information infrastructure custodians in order to evaluate the effectiveness of response plan through lessons learned.

5.7 Cooperation and Partnership

5.7.2 The ngCERT under the framework of National Cybersecurity Coordinating Center will coordinate activities of other sectorial CERT and facilitates cooperation and partnership of all cybersecurity stakeholders, including international and multilateral organizations.

5.7.3 It is imperative to note that, sharing of action noteworthy information about new threats and vulnerabilities with partners by ngCERT will avail them the security status of the national cyberspace and the need to protect it

5.7.4 NgCERT also will enable both government and private sector actors through stimulated exercises to support stakeholders understand their roles during a crisis and better prepare for incident response scenarios. This will test incident response capabilities and processes created to communicate, collaborate, and restore services in the event of an incident.

5.8 Capacity Building

5.8.2 To sustain an optimal incident response readiness capability, technical and procedural capacity building will be instituted for both law enforcement as well as judicial officers to build their expertise and facilitate understanding of the dynamics of cybercrime.

5.8.3 Training will focus on methods of handling digital evidence to ensure that it preserves its evidential weight and thus admissibility in Court.

5.9 National Digital Forensic Mechanism

5.9.1 The National Cybersecurity Coordinating Center shall develop a framework for the setting up of a National Digital Forensic Laboratory as a core unit under the coordination of NCCC.

5.9.2 The implementation and coordination of digital forensic technical and management guidelines will help develop guide for the law enforcement and security agency engagement in digital forensic investigation, analysis, interpretation and reconstruction of e-crime scene.

CHAPTER SIX

STRATEGY ON CRITICAL INFORMATION INFRASTRUCTURES PROTECTION & RESILIENCE

6.1 Introduction

6.1.1 This Strategy articulates the various Critical Information Infrastructure (CII) protection and resilience activities the Government undertakes, ranging from how it engages with business, government (international and domestic) as well as other stakeholders.

6.1.2 This Strategy presents the Government's approach to Critical Information Infrastructure Protection and Resilience (CIIPR).

6.1.3 It also acknowledges that CIIPR is a shared responsibility across governments, the owners and operators of critical infrastructure.

6.2 Vision of CIIPR

- To ensure continued operation of CII in the face of all hazards, as this critical infrastructure supports national defense and security, and underpins our economic prosperity and social wellbeing.

6.3 Mission of CIIPR

- To harness all relevant stakeholder's CIIPR Programs into a national holistic agenda capable of supporting the country's national security and ensure provision of essential services.

6.4 Strategic Objectives

- i. Assess threats to, vulnerabilities of, and consequences to critical infrastructure through an intelligent and information-led, risk management approach.
- ii. Secure CII against physical, human and cyber threats through sustainable efforts to reduce risk.
- iii. Enhance CII resilience by reducing impact of unforeseen and unexpected incidents through advance planning and mitigation efforts, as well as effective responses aimed at saving lives and ensuring rapid recovery of essential services;
- iv. Share relevant information across the CII community to build awareness and enable a coordinated risk- informed decision making, while promoting a learning and adaptation during and after exercises and incidents impacting on CII.
- v. These objectives will be supported by regular developments of more specific priorities by key critical infrastructure partnerships related to risk management and capability enhancement.
- vi. Based on the vision, mission, and goals, the critical infrastructure community will work together to set specific national priorities. National priorities will be set considering resource availability, progress already made, known capability gaps, and emerging trends and risks in cybersecurity.

- vii. National priorities will drive implementation and will be supplemented by sector, regional, and corporate priorities. Performance measures will be set based on the goals and priorities of each sector, regional or national Government.
- viii. The National Annual Preparedness Report will include measurements of progress that will help derive a common understanding of the state of critical infrastructure security and resilient efforts.

6.5 STRATEGIC IMPERATIVES TO ACHIEVE AIMS AND OBJECTIVES

6.5.1 The Government recognizes the importance of critical infrastructure, including those parts that provide essential services for everyday life (such as energy, food, water, transport, communications, health and banking and finance). A disruption to critical infrastructure could have a range of serious implications for business, governments and our social wellbeing.

6.6 Initiative 1: Operate an effective business-government partnership with critical infrastructure owners and operators.

- A significant proportion of the nation's critical infrastructure is privately owned or operated on a commercial basis.
- A business-government partnership will be established to help build confidence and reliability for the continued operation of critical infrastructure that supports national security, economic prosperity, and social and community wellbeing.
- It is important that the business-government partnership offers value and mutual benefit to the parties involved.

6.6.1 Necessity for Trust Information Sharing Network (TISN) Activity for NCIIPP

- There will be need for the establishment of a TISN for National Critical Information Infrastructure Protection Plan (NCIIPP).
- This network will comprise of relevant private sector and government representatives, to raise the awareness of risks to critical information infrastructure, share information and techniques required to assess and mitigate risks, and build resilience capacity within entities in the network.
- Working with the TISN, the private sector is able to bring issues to government that are seen as impediments to achieving critical information infrastructure protect.
- The TISN will be the most visible component of the public-private partnership and will provide an important mechanism to foster cooperation between public- private stakeholders on mutually important issues.
- The TISN will raise awareness on critical infrastructure issues, including potential impediments to achieving CIP. Government agencies directly involved in CIP are able to better represent stakeholder interests in the various machineries of government that are used to develop and implement Government policy and act as critical infrastructure advocates in the broader policy debate.
- Accordingly, Government agencies that have a role in implementing the CIP Strategy are able to influence or shape government policy initiatives that have impact on critical infrastructure organizations and their ability to achieve CIP.

6.6.2 Trusted Information Sharing Network Initiative (TISN)

- The TISN will be established in the Office of the National Security Adviser as an exclusive forum in which the owners and operators of critical infrastructure work come together and share information on threats and vulnerabilities as well as develop strategies and solutions to mitigate risk to the nation's CII.
- TISN members include owners and operators of critical infrastructure, Federal, State and local government agency representatives as well as departments and agencies of government.
- The TISN, through its Sector and Expert Advisory Groups, will promote infrastructure protection to owners and operators as well as promote the need for investment in resilient and reliable infrastructure.

6.6.3 Sector Groups

- Sector Groups form the bridge between government and the individual owners and operators of Nigeria's critical infrastructure.
- Their purpose is to assist owners and operators to share information on issues relating to generic threats, vulnerabilities and to identify appropriate measures and strategies to mitigate risk.

6.6.4 Sector Specific Plans

- There will be sector specific plans for each sector which will highlight sector level performance objectives and feedback to the coordinating agency of government charged with the responsibility of managing the sector.
- For example, the sector specific plan for the Information Technology Sector will be coordinated and managed by the Ministry of Information and Communication Technology. In collaboration with other stakeholders

(public and private sector partners), this Ministry will develop and implement a Sector-Specific Plan (SSP) to enable assessment of national, cross sector critical infrastructure protection and resilience plan. *(Please see appendices pages for a sample approach to implementing sector specific plan and program).*

- Sector specific plan will be developed for other critical infrastructure sectors including but not limited to:

Communications Sector	Government Facilities Sector
Manufacturing Sector	Dams Sector
Defence Sector	Chemical Sector
Power and Energy Sector	Commercial Facilities Sector
Financial Services Sector	Food and Agriculture Sector
Emergency Services Sector	Transportation Systems Sector
Public Health and Healthcare Sector	Water & Waste Water systems
Information Technology Sector	

6.7 Initiative 2: Identifying and Evaluating Potential Critical information Infrastructure

6.7.1 Identification

- There will be national, sectorial and organizational approach in identifying and refining actual and potential critical information infrastructure.
- The National Critical Information Infrastructure Protection Unit of the Office of NSA (NCIIPU) will work with other government agencies, owners and

operators of critical infrastructure to ensure an on-going identification of critical information infrastructure.

- Due to infrastructure investment and expansion, advent of new technologies, population growth and increasing interdependence of systems and technologies, identification process will be subject to continual review.

6.7.2 Evaluation

- After the identification of potential critical components of information infrastructure, there will be the need for the evaluation to understand the mode of operation and estimate its risk levels and criticality.
- The evaluation process relies on the cooperation of infrastructure owners and operators. Having an understanding of the estimated risk and criticality levels is important for the government. However, this does not replace the owner's responsibility to develop a robust risk management program to safeguard their assets from known and unknown threats.

6.8 Initiative 3: Enhancing Strategic Readiness of Infrastructure Owners and Operators

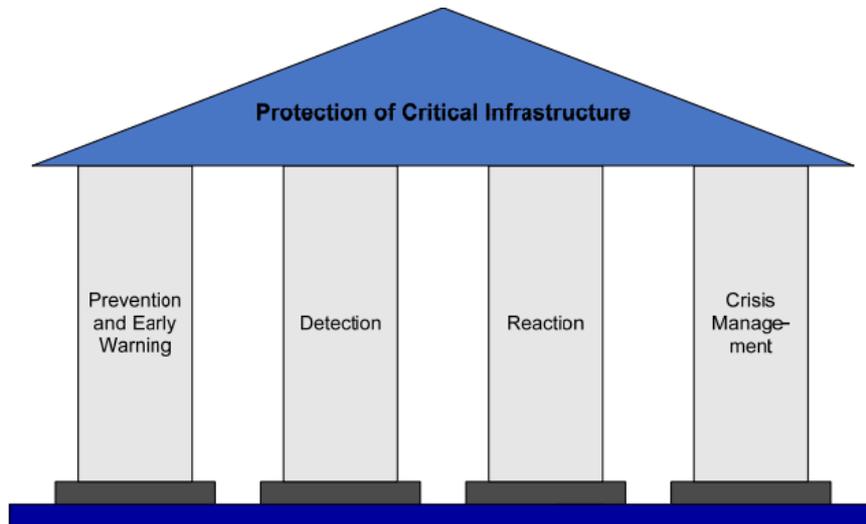
- A key component of the NCIIPP is to sensitize owners and operators to adopt best practices in their approach to planning and preparedness. This will ensure a structured, logical and rigorous approach on the most appropriate steps to take in order to prevent, detect, react and recover from any incident of potential disruptive value.

- Strategic readiness will enable owners and operators identify vulnerabilities and interdependencies as well as plan redundancy programmes including risks from acts of terrorism.

- It is suggested that owners and operators consider the following approach in their preparedness towards enhancing the strategic readiness for protection of critical information infrastructure.
 - i. Prevention and Early Warning Strategy
 - ii. Detection Strategy
 - iii. Reaction Strategy
 - iv. Crisis Management Strategy

READINESS APPROACH TO NCIIPP	
Prevention and Early Warning Strategy	<p>Goal: Ensure CII are less vulnerable to disruptions and impairment duration is short and limited in proportion.</p> <p>Approach: Periodic dissemination of guidelines and best practices on specific threats using the TSIN framework</p>
Detection Strategy	<p>Goal: Discover and detect emerging threats on a timely basis</p> <p>Approach: NCIIPU in collaboration with ngCERT will identify and detect new forms of technical and non-technical attacks</p>
Reaction Strategy	<p>Goal: Identification and correction of causes of disruption.</p> <p>Approach: NCIIPU in collaboration with ngCERT will maintain a 24/7 incident reporting service. Furthermore, distribution of incident report and reaction among TISN members to share lesson learned in improving crisis and emergency planning</p>
Crisis Management Strategy	<p>Goal: Alert key actors of CII of the interdependencies and minimizing effects of disruptions on society.</p>

	Approach: Using TSIN and ngCERT frameworks, constant rehearsals and practice of defined crisis management strategies
--	---



NCSS Figure 5: Four Pillars of Critical Infrastructure Protection [adapted from ITU's A Generic National Framework for Critical Information Infrastructure Protection (CIIP)]

6.9 Initiative 4: Identify, analyse and manage cross-sectorial dependencies

- The identification and analysis of cross-sectorial dependencies assists the risk management decision making of critical infrastructure organizations and helps to inform the Government's policy on CIP.
- Critical infrastructure by nature are highly interdependent, so that failure or disruption in one sector can lead to disruptions in other sectors. For instance, owners and operators of water infrastructure rely on electricity for pumping and telecommunications for monitoring operations. Similarly, the communications industry needs electricity to run their networks, and the electricity industry needs telemetry services to run their operations and electricity marketing.

- A cross-sectorial analysis of dependencies will assist owners and operators of critical infrastructure and the Nigerian Government to understand system-wide risks that are beyond the purview of individual organizations or sectors.
- This increases the potential for a more effective sharing of risk to cope with certain incidents. The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is proposed as a key initiative of the Nigerian Government's efforts to enhance the protection and resilience of critical infrastructure in Nigeria.

6.9.1 The Critical Infrastructure Program for Modelling and Analysis (CIPMA)

- CIPMA is a computer-based capability, which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behavior and dependency relationships of critical infrastructure systems.
- CIPMA uses an all hazards approach to undertake computer modelling to determine the consequences of different disasters and threats (human and natural) to critical infrastructure.
- Owners and operators of critical infrastructure can use this information to prevent, prepare for, respond to or recover from a natural or human-caused hazard.
- CIPMA also helps government shape policies on national security and critical infrastructure resilience.
- CIPMA is an important capability to support the business-government partnership, and relies on strong support from stakeholders such as owners and operators of critical infrastructure, Federal, State and local governments, and government agencies for its ongoing development.

- Importantly, CIPMA can show the relationships and dependencies between critical infrastructure systems, and the cascade impacts from a failure in one sector on the operations of critical infrastructure in other sectors.
- NCIPP unit manages CIPMA and works with ONSA-NCCC and other technical service providers to further develop and deliver this whole-of-government capability.

6.10 Success Criteria And Review Of CIIP Strategy

- Critical infrastructure protection and resilience is an ongoing process that requires periodic review and fine tuning of the activities under each strategic imperative will be required as the strategy is implemented.

6.10.1 Mechanism for Measuring Success:

Success will be measured through following mechanisms:

- Effective Critical Information Infrastructure Protection is reliant on a strong, collaborative partnership between governments and critical infrastructure owners and operators to deliver the Government's policy aim of the continued operation of critical infrastructure in the face of all cyber threats.
- Need for investment in resilient, robust infrastructure (e.g CIPMA) to identify key cross-sectorial dependencies and vulnerabilities with respect to both cyber and physical infrastructure.
- Businesses and governments collaborating to progress national research and submission of curriculum inputs to training and research on CIP
- Periodic lessons from incident report and reaction exercise activities and real life events propagated to all Sector Groups to enhance organization's

- Understanding of protection and resilience and improve planning arrangements.
- Coordination of Nigeria's international engagement with periodic updates provided to NCCC as required
- In order to ensure Government's policy settings remain appropriate, the CIP Strategy will undergo a comprehensive review after five years of operation.

Chapter Seven

STRATEGY ON ASSURANCE & MONITORING

7.1 Introduction

- 7.1.1 There is a need to address the issues of cyber threats from risks management and process governance approaches because of the need to address the nation's internal vulnerability and other weakest link.
- 7.1.2 The development of a National Cybersecurity Strategy designed to address these issues however, is only as good as the National Cybersecurity program that implements it.
- 7.1.3 The continuous monitoring and review (i.e. assessment and evaluation) of the implementation and management of the National Cybersecurity Program, and the surrounding context that it operates within, will be critical in providing assurance to various stakeholders that the National Cybersecurity program is well able, and continually so, to safeguard our vulnerability and other critical national infrastructure.

7.2 Strategic Objective

- i. This strategy seeks to establish and maintain a monitoring and an assurance framework that will ensure that the efforts put in place to secure the nation's cyberspace are in compliance with international best practices, perform as expected by the stakeholders involved, as well as to maintain the capabilities necessary to protect our nation's cyberspace and other critical infrastructure.
- ii. To harness, profile, harmonize and prioritize various technology neutral information security frameworks that will help determine best standards and guidelines suitable to the national peculiarity and in line with international best practices.
- iii. To achieve coordination of information security regimes through consensus, collaboration, and partnership with relevant stakeholders.
- iv. To facilitate national awareness on the criticality of ensuring and enabling information security conscious operational environment both in the public and private sectors

7.3 The Cybersecurity Assurance context

- The surrounding context within which the cybersecurity assurance mechanism will operate and monitor include the following:

- i. The National Cybersecurity Strategy**

This is the foundation on which the National Cybersecurity Assurance Program and action plans will be built, it will be periodically reviewed to provide assurance that will continue to address evolving threats in a dynamic threat environment.

- ii. Stakeholders' Commitment to Cybersecurity**

- An effective and efficient National Cybersecurity Assurance Program will require clear direction, commitment from the highest level of Government, top management and administration executive among others.
- The "tone at the top" will determine to a large extent the commitment shown by others in the lower cadres as it relates to Cybersecurity and also the resources committed to effecting the Program. This will be periodically reviewed and adequate strategies developed to ensure that those at the top are motivated to ensure consistent commitment to the cause of Cybersecurity.

iii. **Cybersecurity awareness level**

- The level to which all citizens of the country become aware of, and educated about cybersecurity issues will to a large extent determine how strong the cybersecurity efforts of the nation will be. As security is only as strong as its weakest link. Initiatives to continually create awareness among the citizens will be established and continually reviewed for effectiveness.

iv. **The Regulatory/Legal environment**

- The Cybersecurity bill, National Cyber Security Policy and other laws, policies and regulations will be periodically reviewed to ensure that they continue to be relevant, properly streamlined and serve as a good legal foundation to support the initiatives to secure the nation's cyberspace.

v. **Cybersecurity Capabilities, Skills, Expertise**

- The level of skills, capabilities and expertise possessed by the personnel that will be charged with the responsibility of securing the nation's cyberspace, who will essentially be Nigerian citizens, will go a long way in determining how well it will be done.

- 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 as related to the skills required to continually defend our nation in cyberspace will be periodically assessed and recommendations made to address any shortcoming.

vi. Risk Management Program

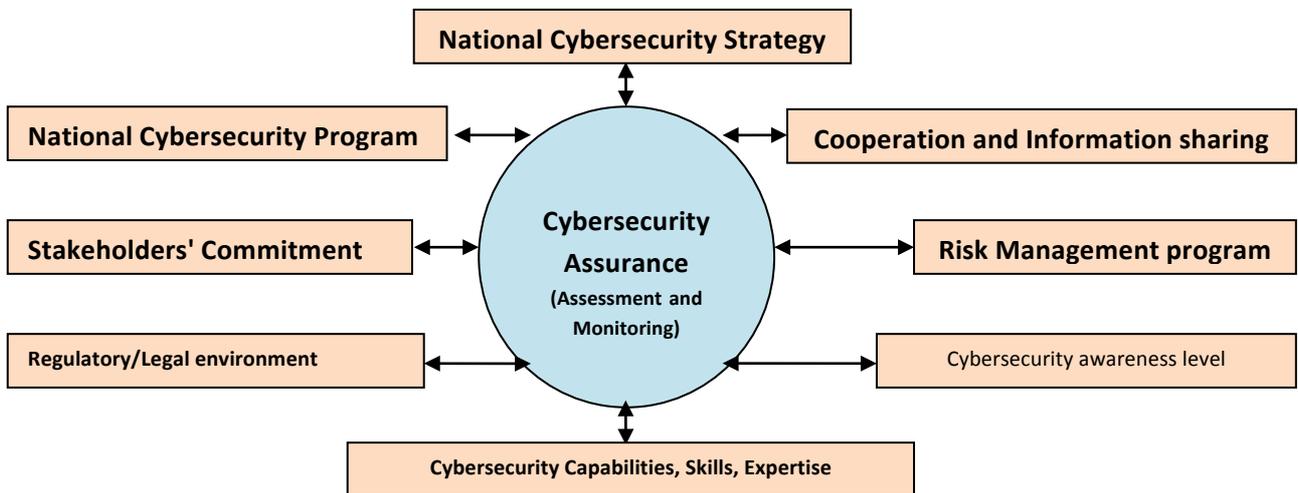
- An effective cybersecurity risk management process will enable the nation to identify, assess, and mitigate risks to the nation's cyberspace. These will include threat analysis both for determining evolving threats to the nation's cyberspace and emerging trends and threats.
- These information feeds into the Cybersecurity program to ensure that it continues to provide countermeasures that will protect the nation against both current and future threats to the nation's cyberspace and also serve as a basis for prioritizing responses to such threats based on risk/impact level.
- The Risk Management program will be established and continually reassessed to ensure it continues to provide relevant information to help proactively protect our presence in cyberspace.

**v. Cooperation/Collaboration and Communication/
Information sharing**

- Level of Public-Private collaboration, intergovernmental, inter-sectorial and international collaboration and communication will continually be assessed to ensure that maximum benefits that leads to a more secure cyberspace are achieved from such collaboration/cooperation and information sharing.

viii **National Cybersecurity program**

Assurance activities including periodic assessment and reviews will be carried out to provide assurance that the cybersecurity program is achieving its objectives and that such objectives will aligned with SMART framework i.e. Specific, Measurable, Achievable, Results-focused and Time-bound



NCSS Figure 6 The Cybersecurity Assurance context - It shows the logical environment within which the Cybersecurity Assurance mechanism will operate and monitor.

7.4 Focal Points

- 7.4.1 Monitor the implementation program for the Cyber Security Strategy to provide assurance that the program is meeting, and will continue to meet stakeholder's expectations within a dynamic cyber landscape.
- 7.4.2 Make recommendations on possible improvements in the Cyber Security Strategy itself based on observed changes in threats profile.
- 7.4.3 Encourage, monitor and review the adoption of national and international best practices as codified in the international frameworks and standards to ensure

national cybersecurity practices that compare well with international standards and practices and also serve as a basis for benchmarking our maturity level.

7.4.4 Monitor and review cybersecurity capabilities of actors at the national, state and sectorial levels to ensure continuous improvement and development of relevant capabilities, skills and proficiencies, enabling them to defend our nation in the face of present and future threats to the nation's cyberspace.

7.4.5 Monitor and review level of preparedness and capacity of various actors at the national, state and sectorial levels to ensure their readiness to defend our nation in the face of present and future threats to the nation's cyberspace.

7.4.6 Ensure a continuous improvement process for cybersecurity.

7.4.7 To develop performance measures both at the policy, strategic, tactical and operational levels based on the proposed Cybersecurity balanced scorecard and perform reviews based on these measures to ensure feedback on performance of the National Cybersecurity program so that adequate corrective and improvement changes can be made.

7.4.8 Conducting information security audits and process audits for government entities and also coordinating and validating security audits and process audits of self- assessment entities.

7.4.9 Conducting and coordinating information security risk assessment and analysis while establishing reasonable security guidelines and measures to protect data and systems.

7.5 Strategy

7.5.1 Initiative 1

- The National Cybersecurity Assurance Department as an arm of the NCCC will be established to serve as a mechanism for fulfilling all Assurance and Monitoring focal points.

- The department will be charged with the responsibilities of providing assurance as regards the National Cybersecurity program.
- The unit will be set up at the start of implementation of the National Cybersecurity program.

7.5.2 Initiative 2

- The Strategy approach to cybersecurity governance is anchored on a sound technology neutral framework. This is in line with global best practice, while emphasizing the need for an effective business governance process from a risk management approach.
- The dynamism of cybersecurity risks requires a flexible and responsive risk management strategy.
- Thus, this Strategy provides adoptable and adaptable fit-for-purpose International Standards and frameworks for information Security Governance, Risk and Control in line with global consensus.
- This strategy will facilitate cooperation among stakeholders responsible for ensuring the security and safety of our cyberspace and other critical infrastructure towards ensuring commonality in approaches to cybersecurity and standardization.
- This initiative recommends consensus driven international standards and multi-stakeholders' frameworks on information security assurance.

7.5.3. Initiative 3

- With a definite timeline, the strategy will implement continuous monitoring software solutions for vulnerability and security configuration compliance monitoring, threat management functions and penetration testing activities to

identify alterations and weaknesses in security configurations on critical national infrastructure.

7.5.4 Initiative 4

- An effective Cybersecurity risk assessment program will be established with a definite timeline.

7.5.5. Initiative 5

- This strategy will implement a core assurance capability thus enabling the nation to assess the effectiveness and adequacy of cybersecurity controls, when evaluated from an attacker's perspective, to deny the compromise of critical nation infrastructure.

7.5.6. Initiative 6

- The Strategy implements an Enterprise Application Security Testing regimen with standardized processes and procedures within application lifecycle development processes to help identify vulnerabilities and weaknesses in custom and source code, web applications and databases deployed to support cybersecurity in the nation.

7.5.7. Initiative 7

- This strategy recommends the adaptation of Balanced Scorecard framework and approach to organization's cybersecurity known as the National Cybersecurity Balanced Scorecard framework. This will serve as the basis of developing performance metrics, key performance indicator (KPIs) and key goal indicators (KGIs) that will be used to measure the success of the Cybersecurity program.

7.5.8. Initiative 8

- This strategy provides for the design, development and documentation of a National Enterprise Security Architecture Framework that will serve as the basis for the design and continuous improvement of a cohesive, standardized and well integrated infrastructure put in place to safeguard the nation's cyberspace

7.5.9. Initiative 9

- Develop Blue team and Red team capabilities among cybersecurity actors.

CHAPTER EIGHT

NATIONAL CYBERSECURITY SKILL & MANPOWER DEVELOPMENT

8.1 Introduction:

Nigeria presently lacks sufficient specialised cybersecurity skilled personnel required for driving national cybersecurity capabilities and empowerment. This national cybersecurity strategy provides for a coherent and coordinated cybersecurity skills and human empowerment framework as envisioned in the National Cybersecurity Policy.

8.2 Objectives:

Cybersecurity skills development is a national priority and also a foundation for the achievement of national cybersecurity readiness. Therefore, this focus area aims to achieve the following objectives:

- i. To provide an institutional framework anchors on public-private partnership towards building local professional skills.
- ii. To provide central coordination and regulation of skills development within the public sector.
- iii. To help build framework for public-private partnership on professional training and capacity building in cybersecurity for private sector

towards promoting common understanding on cybersecurity challenge.

8.3 Scope

8.3.1 The scope of the national cybersecurity skills development include the following;

- i. To leverage on cybersecurity in national security and economic innovation for competitive advantage.
- ii. To develop cybersecurity professional skills roadmap that will facilitate emergence of local content and expertise.
- iii. To harness initiatives that will stimulate emergence of cybersecurity industry in Nigeria.

8.3.2 Therefore, this section focuses on the framework for the creation of programmes to increase the cadre of cybersecurity professionals in Managerial, Technical and Information Assurance areas rather than general user awareness and education. It further advocate for re-organization of the nation's educational priorities to address cybersecurity challenges and opportunities.

8.4 Initiatives

8.4.1 A specialized national skills development and empowerment initiative on cybersecurity covering various level of knowledge in information assurance will be established under the National Cybersecurity Coordinating Center.

- The initiative will be set up under the framework of Nigeria Institution of Cybersecurity (NIOC) in partnership with stakeholders as enshrined in the National Cybersecurity Policy.
 - The framework will involve designing, developing, and implementing level of skills, requirement, coordination, certifications, regulations, capabilities and expertise to be possessed by the personnel that will be charged with

the responsibility of securing and maintaining the nation's presence in cyberspace, who will essentially be Nigerian citizens.

- 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.

8.5 Roadmap for Nigeria Cybersecurity Industry:

- 8.5.1 In Nigeria, cybersecurity essential skills at the public institutions and industry level engagement are scarce. The scarcely available ones are extremely limited in their scope and capabilities to safeguard and protect critical industries. Various genuine concerns have been expressed on the apparently incapacity of Nigeria as a nation to protect itself and her industry in the face of a major attacks on her Critical Information and Related Infrastructures.
- 8.5.2 Stakeholders from Industries, law enforcement agencies, academics, non-governmental organizations, government Ministries, Department and Agencies, Nigeria Professionals in diasporas should emerge together under a proposed framework for cybersecurity profession umbrella body to help the country drive common professional synergy on cybersecurity instrument of research and development, innovations, and trusted cooperation necessary for a national cohesion on cybersecurity.
- 8.5.3 The proposed government and private sector synergy should culminate into the formation of Nigeria Institution of Cybersecurity (NIOC) that will help develop and drive a coherent body of useful and applicable knowledge in cybersecurity.
- 8.5.4 The NIOC will be expected to be built on nationwide standards with the aim of harmonizing, developing, promoting and enhancing multidisciplinary professional skills capacity and standards in the development of Cybersecurity industry, while providing opportunity for the citizen positive engagement in cyberspace.
- 8.5.5 It is expected that by promoting national dignity, preserving national security and economic values, including international standards on multidisciplinary professionalism and expertise, the institution will serve the human resources needs of the country in both the government and private sectors covering all

aspect of cybersecurity as defined through the international framework of cooperation on cybersecurity and other widely recognized international best practices.

Source: Recommendation from 1st National Conference on Cybercrime & Cybersecurity 2008 –An event organised by Global Network for Cybersolution in collaboration with NITDA, NCC, Ministry of Justice

8.6 Institutional Framework

- 8.6.1 Under the NCCC, NIOC will provide strategic framework for partnership with the following stakeholder on cybersecurity skill development, creativity, innovation and research: academia, research & development agencies, industry, and multi-stakeholder civil society.
- 8.6.2 The NIOC will develop professional career standard, minimum entry requirement, based on categorizations acceptable to the government and local industry.
- 8.6.3 It will develop unified scheme for national certifications, training in cybersecurity, capacity building and granting recognized professional status level correspondence to professional categorization.
- 8.6.4 NIOC will develop professional syllabus standardizations, and prospectus for short term and career focused professional skills development.
- 8.6.5 NIOC will prepare, coordinate, regulate and conduct NIOC professional examinations in different categories of certification nationwide in collaboration with the industry.
- 8.6.6 The NIOC will regulate, approve and coordinate the lists of independent and accredited cybersecurity training centres in the country.
- 8.6.7 NIOC will provide professional guidelines in learning resources, materials and curriculum development that best meet local and international requirement.
- 8.6.8 NIOC will provide professional measurable benefits in line with national and international best practices to all professional members scalable to fit into various categories of membership.
- 8.6.9 NIOC will develop industry acceptable waiver schemes or conversion programs for relevant established professionals interested in cybersecurity profession, Public institutions, law enforcement agencies, Military, Para-military and security agencies whose operation and experience are relevant to cybersecurity irrespective of the professional background.
- 8.6.10 NIOC will develop industry acceptable waiver schemes or conversion programs for relevant established academics in the field of law, ICT, IT,

Finances and relevant to the field of cybersecurity specialization, research and development.

- 8.6.11 NIOC will develop industry acceptable conversion programs for young Nigeria graduates in any recognized and approved discipline or, and equivalent in line with the NIOC approved levels of certifications and categorization of membership.
- 8.6.12 NIOC will promote federal government and industry acceptance of certifications Nation-wide.
- 8.6.13 NIOC will develop strictest professional code of ethical conducts, professional dispute and conflict resolution structures.
- 8.6.14 NIOC will secure international best practices approval and relevant international standards from global institutions.
- 8.6.15 NIOC will provide framework for continuous professional development in line with international best practices.
- 8.6.16 NIOC will interface and collaborate with relevant and other related professional bodies for technical cooperation and partnership on technical exchange programs relevant to cybersecurity.
- 8.6.17 The NIOC professional training and skills development will be based and focused on generic cybersecurity technology and tested models as adopted globally.
- 8.6.18 NIOC will become a unifying professional body accommodating all cybersecurity stakeholders from existing professional bodies in the country whose professional engagement fall within the purview of NIOC.

Securing Nigeria in Cyberspace:

To build an infinitely sustainable cybersecurity readiness, there is critical need to focus on our collective strength, sense of responsibility, excellence, prudence, and strategic appropriation of our collective ingenuity for the benefit of protecting our common wealth in cyberspace within the current and future dispensation.

CHAPTER NINE

STRATEGY ON ONLINE CHILD ABUSE & EXPLOITATIONS

9.1 Introduction:

- Cyberspace has brought huge benefits to children around the world, with the number of connected households increasing each year. While the potential for good is undisputed, Internet has become increasingly accessible to the critical segment of our population i.e. Nigerian children and young people, both at home and in schools.
- Rather than surfing the Internet passively, children and young people participate in a dynamic online environment that allows them to generate, manipulate and consume internet content like never before, forging their place and identity in online communities.
- More importantly, as a result of the universal availability of Internet access in homes, schools, libraries, mobile phones, etc., children are increasingly becoming involved in the use of the new technological application and taking advantage of the opportunity it provides for learning, research, entertainment and business.
- However, the Internet has also raised new and disturbing issues of vulnerability, especially for children. It exposes children to potentially negative contents.
- Children and Young Persons are the most active participants in online social networking and therefore are potential victims of improperly disseminated and dysfunctional contents that could cause disorientation and threaten their survival and that of the society.
- There are growing concerns on the distribution of online child abuse materials targeted to children which are making them vulnerable to child pornography, sexual abuse, harassment, exploitation, extremism, brain washing for terrorist

acts of violence and human trafficking resulting into unpleasant outcome of the information age.

- In order to address these issues of child online exploitation and its disastrous consequences, the National Cybersecurity Policy viewed it as one of the critical areas of focus.

9.2 Rationale for COAEP

9.2.1 The National Cybersecurity Policy framework provides a rationale and philosophy to guide development of strategy for Nigerian Child Online Abuse and Exploitation.

9.2.2 The Principles on Child Online Abuse & Exploitation and Counter-measures emphasized Social Media as a vital attractive channel and tool for social interactions and productive engagements. Regrettably, the openness and transparent nature of cyberspace have been exploited for good causes and malicious intents.

9.2.3 Therefore, there is need for the following actions;

- i. Integration of Child Online Abuse and Exploitation into National legislation on cybercrime and cybersecurity.
- ii. There is a need to establish that any act against a child which is illegal in the real world is illegal online and that online data protection and privacy rules for legal minor are also adequate.
- iii. Ensure that a mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the internet , for example , a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible

9.2.4 It is the intention of government to harness counter-measures through a legislative framework, policy and strategic actions to address cyber abuse and online exploitation of Nigerian Child in a manner that will prevent and curtail cybercriminal intents and related malicious acts inimical to the national dignity, security and economic interests of the country.

9.3 Objectives

9.3.1 To provide common approach in the development and implementation of National Countermeasures strategy.

- 9.3.2 To provide robust security initiatives, action plan, and roadmap that will give overall direction to the planning and implementation of these countermeasures strategy within the framework of National Security.
- 9.3.3 The strategy addresses urgent security and law enforcement challenges, roles and shared responsibilities and government interventions.
- 9.3.4 The strategy harnesses frameworks that provide coherent structure for coordination of multi stakeholder engagement.

9.4 Strategic Approach

These objectives are anchored through the following approaches while considering our socio-economic security peculiarity and vulnerable operating environment for the purpose of protecting Nigerian children and young generations on the internet.

- i. The National Cybersecurity Strategy approach adopts multi-stakeholder and multi-sectorial collaboration through partnership and alliances of government and key actors with clearly defined and specific guidelines for policy makers, law enforcement and security agencies.
- ii. The partnership and alliances will be forged to ensure cooperation for action and mutual awareness among stakeholders on the consequence of improper engagement in cyberspace.

9.5 Strategy

9.5.1 Initiative 1: Focusing on National Process Mechanism

- i. There shall be Infusion of Child Online Abuse and Exploitation Protection Strategy (COAEPS) into the larger framework for National cooperation on cybersecurity.
- ii. Establishment of a unit under the National Cybersecurity Coordinating Center (NCCC) to handle matters relating to Child Online Abuse and Exploitation within the scope National Cybersecurity Policy.
- iii. The COAEP unit of NCCC will collaborate with industry regulators and operators to implement a coherent Countermeasures Technical Mechanisms (CTM) to prevent access to web sites identified as hosting

contents that are offensive to children and to implement processes to enable the removal of any child sexual abuse content posted on their own services.

- iv. The Unit will provide partnership mechanism in regard to the promotion of public awareness, messages and campaigns center on safety and security of Nigeria children interactions online.
- v. The unit will train and build the capacity of Nigerian Law enforcement officers to conduct investigations into Internet related crimes against children and young people and maintain a register of convicted online crime offenders.
- vi. The unit will facilitate national processes which ensure that all Child Abuse and Exploitation materials found in cyberspace are channeled towards a centralized, national resource.

9.5.2 Initiative 2: Focusing on International Process Mechanism

- i. The NCCC will drive Virtual National Taskforce (VNT) which will work with *Virtual Global Taskforce*, a law enforcement body which provides a 24/7 mechanism to receive reports about illegal behavior or content from persons across the globe. The nation will develop modality for working with this global security platform most especially for countermeasures against terrorist recruitment and online predators.³
- ii. It is strategically essential that the Nigerian law enforcement community becomes fully informed through training and capacity building and empower through legislation to help make the Internet safer for children and young people.
- iii. Investing in training for law enforcement, prosecutorial and building capacity of Nigerian Judges through collaboration with National Judiciary Institutes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices on Child Abuse Materials.

9.6 Operational Measures

³ www.virtualglobaltaskforce.com

- 9.6.1 NCCC will ensure that a working mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the Internet, for example, a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible.
- 9.6.2 NCCC will ensure various security and law enforcement agencies in the country implement abuse report mechanisms which will be prominently displayed on relevant parts of any web site that allows user generated content to appear. It should also be possible for people who feel threatened in any way, or for people who have witnessed any worrying activity on the Internet, to be able to report it as quickly as possible to the relevant law enforcement agencies that need to be trained and ready to respond.
- 9.6.3 NCCC will promote a number of software programmes which can help screen out unwanted material or block unwanted contacts. Utilizing some of the child safety and filtering programmes because they are part of a computer's operating system or they are provided as part of a package available from an ISP or ESP. The manufacturers of some game consoles also provide similar tools if the device is Internet enabled. These programmes are not foolproof but they can provide a welcome level of support, particularly in families with younger children. These technical tools will be used as part of a broader arsenal. Parental and/or guardian involvement is critical.
- 9.6.4 It is strategically essential that the Nigerian law enforcement community becomes fully engaged with any overall strategy to help make the Internet safer for children and young people.
- 9.6.5 Nigerian Law enforcement officers will be appropriately trained to conduct investigations into Internet related crimes against children and young people. They need the right level of technical knowledge and access to forensic facilities to enable them to extract and interpret data obtained from computers or the Internet.
- 9.6.6 NCCC will establish a clear mechanism to enable children and young people, or any member of the public, to report any incidents or concerns they might have about a child's or a young person's online safety.

9.7 National Security Response Measures

- 9.7.1 With escalation of cybercrime, youths based conflict and terrorist recruitment, bombing attack in the country, the Internet has made possible a range of

ways of abusing children and recruiting young people, e.g., through web cams, chat rooms and internet blog.

9.7.2 The internet has also played a singular role in expanding the scale on which Child Abuse Material (CAM) has become available in all parts of the world. For these reasons, when addressing online safety concerns for children and young people from national security perspective, the Strategy gives special consideration to the following:

- i. Outlawing “grooming” or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity, possession, production and distribution of CAM, irrespective of the intent to distribute.
- ii. Taking additional response steps to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM.
- iii. Ensuring that national processes are in place which ensure that all CAM found in a country is channeled towards a centralized, national resource.
- iv. Developing strategies to address the demand for CAM particularly among those who have convictions for such offences. It is important to build awareness of the fact that this is not a victimless crime: children are abused to produce the material being viewed and by intentionally viewing or downloading CAM one is contributing directly to the abuse of the child depicted and one is also encouraging the abuse of more children to produce more pictures.
- v. Building awareness of the fact that Nigerian children usually would not consent to being sexually abused, whether for the production of CAM or in any other way. Encourage people who use CAM to seek help, while at the same time, making them aware that they will be held criminally responsible for the illegal activity in which they engaged/are engaging.
- vi. Ensuring that law enforcement crime prevention strategies as well as school-based and social programmes include sections on cyber safety and the risks posed by online predatory behavior, with age appropriate advice.

- vii. NCCC maintains a register of convicted online crime offenders. Courts have issued judicial orders banning such offenders from using the Internet altogether or from using parts of the Internet which are frequented by children and young people. The problem with these orders hitherto has been its enforcement.
- viii. Consideration will be given to integrating the list of convicted sex offenders into a block list which will prevent those on it from visiting or joining certain web sites.
- ix. Providing appropriate long term support for victims. Where children or young people have been victimized online, where for example an illegal image of them has appeared on the Internet, they will naturally feel very concerned about who might have seen it and what impact this will have on them. It could leave the child or young person feeling vulnerable to bullying or to further sexual exploitation and abuse.
- x. Ensuring that a grassroots' reporting and intelligence gathering mechanism is established and is widely promoted to provide a readily understood and rapid means for reporting illegal content or illegal or worrying online behavior e.g. a system similar to that which has been established by the Virtual Global Taskforce. The use of the INTERPOLi24/7 system will be encouraged.
- xi. Ensuring that a sufficient number of law enforcement officials are appropriately trained in investigating Internet and computer-based crime and have access to appropriate forensic facilities to enable them extract and interpret relevant digital data.
- xii. Investing in training for law enforcement, prosecutorial and judicial authorities in the methods used by online criminals to perpetrate these crimes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices.
- xiii. In addition, it will be important to establish bilateral and multilateral collaboration and information exchanges with relevant law enforcement authorities and investigative bodies in other countries.

CHAPTER TEN

STRATEGY ON PUBLIC-PRIVATE PARTNERSHIP

10.1 Introduction

- The present administration has demonstrated her commitment to the prevailing security challenges by taking positive step to re-invigorate National Cybersecurity Strategy as part of the National Security agenda.
- The Cybercrime legislation and the need to actualize the implementation of National Cybersecurity Strategy requires effective machinery of public-private partnership and management framework to drive the buildup process with tripartite synergy of the whole nation including the government, non-government actors and international stakeholders.
- In the light of the above, this section seeks to provide the government with a strategic public-partnership management framework approach for the implementation of National Cybersecurity Strategy.
- The key elements of this strategy are as follows:
 - i. The PPP Management Framework to facilitate the cooperation and partnership in the implementation of National Cybersecurity Strategy among the tripartite stakeholders in the country.
 - ii. The Nature of the PPP Framework Model, Benefit, Impact & Direction.
 - iii. Special Purpose Vehicle and Delivery channel through the setting up of PPP for Cyber security (3PC).
 - iv. 3PC Working Document & Terms of Reference
 - v. 3PC Sustainable Strategy

vi. Evaluation & Appraisal

10.2 The Imperative of Public-Private Partnership Framework for National Cybersecurity Strategy

- In the current dispensation, engagement in cyberspace is central to the existence, survivability, relevancy, as well as security and protection of the public institutions and private sector businesses.
- The public and private sectors' interests are enormously intertwined with a shared responsibility for ensuring a secure cyberspace and a protected critical economic infrastructure upon which businesses and government services depend.
- Public-Private Partnership framework is critical to the build-up process and overall success of the National Cybersecurity Strategy.
- Right from the commencement of the efforts on National Cybersecurity Strategy since 2003, which was reinvigorated in 2010 and till the present time. Most often, private sectors are usually caught unprepared in the buildup process.
- There is a concrete evidence that the Federal government cannot succeed in the many facets of securing National cyberspace if it works in isolation in her build up in the implementation of National Cybersecurity Strategy. Therefore PPC is set to define roles and responsibilities, integrate capabilities, and facilitate joint ownership of the problems and the challenges towards developing holistic Cybersecurity Strategy. It is only through such sustainable partnerships that the Country will be able to enthrone cybersecurity and reap the full benefits of the digital revolution.
- Furthermore, the National Security challenge of securing cyberspace requires an increased effort in all stakeholders' collaborations. This effort should seek—in continued collaboration with the private sector—to improve the security of national interoperable networks
- The private sector, however, designs, invest, builds, owns, operates and maintains most of the critical information infrastructures that support government and private users alike.
- Therefore Industry and governments share the responsibility for the

security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies.

- There are various approaches the NCSS take to address these challenges, some of which require changes in law and policy.
- Thus private-sector engagement is required to help address the limitations of law enforcement and national security. The Federal government and the private sector have an enduring interest in assuring the security of the digital infrastructure. Accordingly, government-industry collaboration is fundamental to achieving National Cybersecurity Strategy.
- It is, therefore, critically important that government and private sector work together in a proactive way. Successful government-private sector collaboration requires three important component:

i. **A clear value proposition:**

- NCCC will articulate the mutual benefits to government and private sector partners.

ii. **Clearly defined roles and responsibilities.**

- **NCCC will** develop a framework for common understanding that will guide mutual working relation and define basis of relationship between NCCC and private sector with clearly define roles and responsibilities.

iii. **Trust:**

- This is fundamental and necessary for establishing, developing, and maintaining sharing relationships between government and industry.
- NCCC will develop, engender, nurture and infuse a Trust Framework for public-private sector cooperation and understanding on critical issues of cybersecurity assurance and monitoring, sectorial CERT, and critical information infrastructure protection plan.
- NCCC will provide a Trust Framework that respect and address industry areas of concern in a manner that will not jeopardize but

balance intrinsic business interest and National Interest.

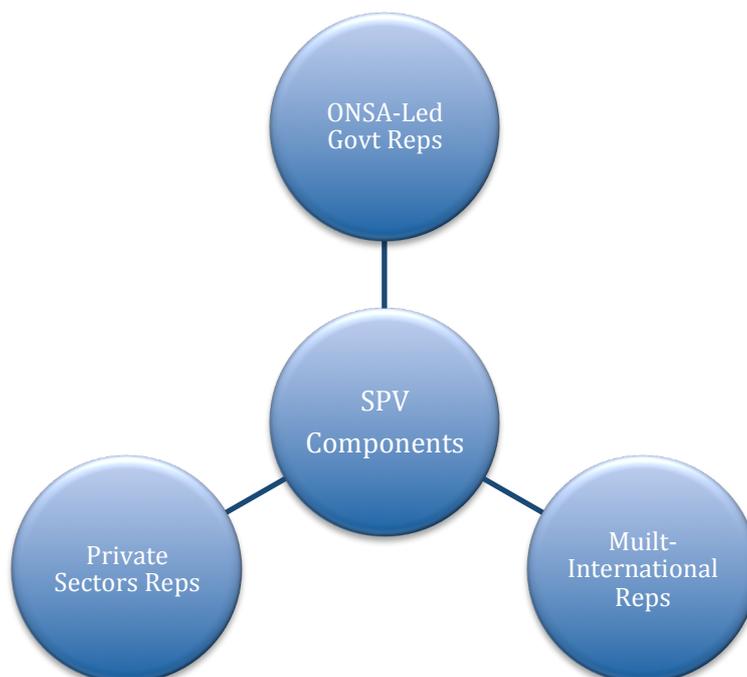
10.3 Public-Private Sector Partnership Management Strategy (PPPMS)

10.3.1 The nature of the proposed PPMF Model involves the following:

- A linear build-up structural processes and national coordination through a PPP Special Purpose Vehicle created by NCCC for this purpose
- The SPV drives and coordinates all the PPP buildup processes for the coordination of government and industry partnership.



Fig 7 The proposed linear build-up process coordination through Special Purpose Vehicle (SPV)



- The ONSA through the NCCC will take the lead by establishing PPP- National Technical Working Group (NTWG) composing of representatives from private sector, government organizations and representatives of international multistakeholder partners.
- The NTWG should not exceed a number needed to be sufficient representatives of all the interests but at the same time capable of conducting PPP-MF business.
- To assure its continued connection to the interests it is intended to represent, provisions could be made for term limits for members.

10.3.2 The Objectives of PPP Management Framework (PPPMF)

- i. To develop and implement public-private partnership action plan to support the review and monitoring of implementation cybercrime and cybersecurity legislation.
- ii. To provide and nurture a sustainable trusted platform for National cooperation, understanding and interactions among all stakeholders, while managing all the build-up processes that will lead to the harmonized agreements on National Cybersecurity among the government, lawmakers, and the private sector.
- iii. To provide a national mechanism that will unify variety of positions, equities, and knowledge gaps to overcome differences and addresses institutional diverse positions.
- iv. To secure other stakeholders inclusion in the development and implementation of National Cybersecurity efforts.
- v. To facilitate the development and coordination of private sector groups from different critical infrastructure industries related to Cybersecurity to address common security interests collaboratively with government.
- vi. To create and nurture trusted forums to address common Cybersecurity challenges, national discourse and dialogue that will enhance cooperation and understanding among various groups on National Cybersecurity effort.
- vii. To institute fundamental arrangements between government and the private sector for Cybersecurity incidence and response management.

10.3.4 Implementation Vehicle for the Public-Private Partnership Management Framework

- i. Creation of PPP-National Technical Working Group (NTWG) for the Implementation of the PPP-Framework.
- ii. The mandate of the NTWG will be anchored on the implementation of PPPMF objectives with the overall mission of actualizing national adoption and operation of National Cybersecurity Strategy within the country.
- iii. A selection criteria for the appointment of the Members of NTWG is based on the value Impact of their respective inputs, in terms of the following;
 - Technical contributions
 - Critical Infrastructural Operators
 - National Platform & Backbone
 - Organizational Support: Structure & Coordination
 - Media
 - Non-government Organization
 - Multi-stakeholder Management
 - Understanding of Regional and Global framework for cooperation
 - Legal Issues
 - Public interest

10.3.5 The Benefit & Outcome of PPP-MF

- i. It provides opportunity for government to effectively engage the core stakeholders in the country while entrenching nationally acceptable National Cybersecurity Strategy at the onset.
- ii. Cybersecurity Strategy is a complex set of issues involving legal, socio-economic, and national security considerations. Several public institutions have significant jurisdictional claim on cybersecurity issues.. The PPPMF will, therefore, provide opportunities to address all the divergent positions of these stakeholders.
- iii. Cybersecurity strategy has a deep connection with critical information infrastructure, economy and security. Private sector provides technology innovations, critical resources and technical standards that the government needs to drive National Cybersecurity Strategy. While government provides enabling mechanisms, instruments and authorities to transform industry best practices and standards into the

framework of National Cybersecurity Strategy, thus, PPPMF will assist government to address structural weaknesses.

- iv. National Cybersecurity Strategy driven through the public-private partnership of government and private sector has greater national security implication and economy protection values, than government working alone or in partnership with multilateral and multinational institutions.
- v. PPPMF enables a trusted platform for strategic information sharing between government and private sector critical for the overall success of National Cybersecurity Strategy.
- vi. It provides partnership vehicle for National Executive Council, National Assembly and private sector to achieve mutual understanding and cooperation on the operation of Cybersecurity legislation and implementation of National Cybersecurity Strategy.
- vii. PPPMF will facilitate structural coordination across the public and private sector, building public confidence in National Cybersecurity Strategy.
- viii. Government depends on a privately operated cyber infrastructure. Through the PPPMF, government engages with industry to continue building the foundation of a trusted partnership. This engagement will build value propositions that are understood by both government and industry partners for the benefit of National Cybersecurity Strategy.

CHAPTER ELEVEN

Strategy on National Internet Safety

11.1 Introduction

- The nation is building various capabilities in computer security emergency response and internet is fast becoming the mainstream for economy and interaction. The government will need to interface with ordinary citizens engaging online on protection awareness, safety consciousness, learning materials, security tools and tips shall be articulated, localized and transmitted online to safeguard the most critical asset of the nation, i.e. her people.
- The Strategy on National Internet Safety is a response to the national need to *plug in* the National Internet Safety capability gap within the currently emerging cybersecurity in the country.
- The initiative fits into the framework of National Cybersecurity Policy, National Security Strategy and National ICT policy.
- The strategy is a product of intensive research, outcome of critical needs assessment, recommendations of various fora and wider consultations on the criticality of public internet safety and online vulnerability in Nigeria.
- During the Nigeria Internet Governance Forum (NIGF 2013), it was estimated that over 95% of Nigerian on the internet are ignorant of personal security and safety responsibility online.
- The weakest link within a cybersecurity chain of any country is her people. Therefore, this Strategy provides initiatives and measures that help safeguard general public internet users, provide materials and facilitate tools to help safeguard Nigerian citizens against cyber threats and unwholesome vulnerability.

- The Strategy is focusing on the development and implementation of National Internet Safety Initiative (NISI) under the structural framework and coordination of NCCC.

11.2 National Internet Safety Initiative

- The initiative is a multi-disciplinary *Initiative* that help safeguard Nigerian citizens' presence on the Internet.
- This is a unique home grown government intervention vehicle which seeks to help the nation protect her citizens against her own digital vulnerability and online threats, safeguards the vulnerable groups, and re-channel her citizens online engagement towards a rewarding experience that impact the socio-economic development and healthy digital lifestyles in cyberspace.
- The initiative is anchored on National Cybersecurity Strategy i.e. the strategy is expected to be built through multi-stakeholder engagement.
- It addresses internet safety and online security from the perspective of local and global peculiarities.
- The strategy marshalled counter-measure policy guidelines, roadmap strategy, local ideas, tested tools and materials for the delivery of the initiative.

11.3 Objective

- The overall objective is to facilitate a unifying Nigeria Internet security literacy programs, open ended, with workable guidelines, and with implementation strategy that will engage Nigerians online and safeguard Nigerian public Internet users.

11.4 Scope:

- The initiative scope is focused on Nigerian public internet users covering the following areas which can hamper National Security, economy growth and local innovations.
 - i. Blacklisting Inappropriate contents
 - ii. Online backdoor distributive channels
 - iii. Misuse and abuse of critical internet resources
 - iv. User abuse and exploitative materials
 - v. Digital vandalism critical to national economic image and online presence
 - vi. Internet security and online safety illiteracy
 - vii. Non-alliance countermeasures

viii. Local peculiarity & literacy gap

11.5 Initiative

- i. Establish a strong NISI presence under an effective multi-stakeholder engagement framework.
- ii. Designate NISI counter-measure advocacy requires to address online security and safety awareness and protection of Nigeria Citizens online.
- iii. Initiate a national road shows- public awareness and education campaign to promote Citizen Online Safety & Protection in Nigeria.
- iv. Setting up NISI hub under NCCC with capability for collaborating Network through which stakeholders can plug-in and interface with tools, materials programs, initiatives within the country.
- v. Build public internet safety emergency readiness, national advocacy and awareness gateway which will fit into the emerging e-security ecosystem thus complimenting existing countermeasure efforts from various government agencies and private sector.
- vi. Development of monitoring tools and evaluation process to help safeguard local internet community and critical presence.
- vii. Building an indigenous capability for local internet presence, security and safety research and development.
- viii. Development of local IT tools, materials, contents and software applications appropriate for ensuring internet security and safety of the citizens.
- ix. Create local Internet Safety Wall using countermeasures awareness, interactions and information sharing.

- x. Establish response mechanism and measures for public alert system

11.6 Importance of NISI to NCCC

- Today, more than ever, government sees a real urgency to get the message out to the community about the emerging threats and abuses of the citizens on the internet. It is within the purview of ONSA through the National Cybersecurity Strategy to provide guidance towards the development of home-grown innovative ideas, tools and materials that will help facilitate internet safety consciousness and online security learning aids to the citizens.
- The initiative is an important focus of NCSS to help design, develop, advocate, train and sustainably deliver resources to government, corporate and individual citizens, families and key players to raise awareness on National Internet safety to make the online community a safe place for productive engagement for government, businesses, kids, young, adult people and families.
- The initiative helps reawaken the nation to its statutory role within the framework of National Cybersecurity Policy towards safeguarding Nigerian Online Presence, developing and implementing local strategies, guidelines and mobilization of all stakeholders to achieve this cause through enterprise and unified platform of National Cybersecurity Coordinating Center.

