NOVEMBER 2017

OFFICE OF THE NATIONAL SECURITY ADVISER

ACTION PLAN FOR IMPLEMENTATION OF THE NATIONAL CYBERSECURITY STRATEGY

Table of Contents

1.0 Executive Summary 2

2.0 INTRODUCTION 3

3.0 PROGRESS ON IMPLEMENTATION OF THE NATIONAL CYBERSECURITY STRATEGY 6

STRATEGY ACTION PLAN 8

3.0 National Cybersecurity Governance, Coordination and Assurance Mechanism 9

4.0 Legal and Regulatory Framework 11

5.0 National Cyber Incident Management Framework 13

6.0 Critical National Information Infrastructure (CNII) Protection and Resilience 15

7.0 Cybersecurity Awareness Campaign, Internet Safety and Child Online Protection 18

8.0 Cybersecurity Capacity Building and Manpower Development 20

9.0 Public Private Partnership 22

APPENDIX A | ABBEREVIATIONS 24

APPENDIX B | DEFINITIONS 27

APPENDIX C | OVERVIEW OF THE NATIONAL CYBERSECURITY STRATEGIC ROADMAP 28

APPENDIX D | NCCC COORDINATION FRAMEWORK SCHEMATIC 29

1.0 EXECUTIVE SUMMARY

1.1 The pervasive applications of the Information and Communication Technology (ICT) means, we live in a hyper-connected world that is increasingly becoming connected on the Internet and its associated information networks and operating space, commonly referred to as the cyberspace. Currently, more than 45% of the world population are connected to the cyberspace, and this number is growing across the globe. In Nigeria, the number of Internet users has grown from less than a million in 2003 to over 80 million in 2017. Consequently, private and public organisations are continuously migrating their operations and services online, just as modern industrial facilities and production systems are also increasingly connected to computer networks for their control and security. As our critical infrastructure continue to connect to computer and information networks; in the nearest future, nations would rely on these networks for essential service delivery. Therefore, the cyberspace has become a driving force for productivity and development, which makes the protection of Critical Information Infrastructure a national security responsibility requiring government, public and private sector to collaborate and synergise.

1.2 On the other hand, increase in Internet connectivity is also associated proliferation of attack vectors, thus, increasing vulnerability of critical systems to attacks by criminals, non-state and state actors. In meeting Government goal of ensuring a secure cyberspace for Nigeria, Section 41 (b) of the Cybercrime (Prohibition, Prevention, etc) Act, 2015 mandates the Office of the National Security Adviser (ONSA) to "ensure formulation and effective implementation of a comprehensive National Cybersesurity Strategy and a National Cybersecurity Policy for Nigeria". In furtherance of this mandate, ONSA has developed an Action for implementing the National Cybersecurity Stratgy. The objective of the Action Plan is to outline government priorities, plan and direction for implementing the strategy. To this end, the draft Action Plan identifies suggested activities, roles and responsibilities of key stakeholders with deliverables, timeline and Key Performance Indicators (KPI) for measuring progress towards effective implementation of the National Cybersecurity Strategy. Furthermore, the document highlights the progress made by various government Ministries, Departments and Agencies (MDAs) towards implementing provisions of the Cybercrime (Prohibition, Prevention, etc) Act, 2015 and the National Cybersecurity Policy and Strategy. To consolidate on this progress, all MDAs and private sector stakeholders are requested to make inputs into the Draft Action Plan in alignment with their statutory mandates. This is with a view to enable government to effectively utilize the numerous potentials inherent in the cyberspace while mitigating the effects of cybercrime and improving safety and security of Nigerians.

2.0 INTRODUCTION

2.1 Increasingly, nations are depending on information and communications technology (ICT) for providing inclusive governance, improved businesses and economic growth. Central to ICT is the Internet and its associated cyberspace with applications that are not limited by physical or geographical boundaries. As it facilitates globalization and drive activities in both critical and non-critical sectors, the cyberspace has become an essential communication medium of the 21st Century and beyond. However, this development comes with inherent threats. The cyberspace can be employed for criminal activities with negative impact on the nation's economy, national security as well as safety and privacy of Nigerians. This reality means the nation must devise strategy to guide Governmental efforts towards creating a secure cyberspace for Nigerians.

2.2 To this end, in February 2015, the Federal Government of Nigeria launched the National Cybersecurity Policy[1] and National Cybersecurity Strategy[2] to provide cohesive measures and strategic actions towards assuring security and protection of the nation's presence in cyberspace. The two documents complement each other on delivering Nigerian Cybersecurity Programs in line with the National Security Strategy 2014[3], through a multi-stakeholder engagement involving government Ministries, Departments and Agencies (MDA), private sector, civil society groups and international partners. This is in compliance with Section 41 of the Cybercrime (Prohibition, Prevention, etc) Act, 2015[4], which assigned to the Office of the National Security Adviser (ONSA), the responsibility to "ensure formulation and effective implementation of a comprehensive National Cybersesurity Strategy and a National Cybersecurity Policy for Nigeria". The National Cybersecurity Strategy identified five (5) key areas of cyber threat inimical to security, economic interests and growth of the nation, namely: *Cybercrime, Cyber-espionage, Cyber-Conflict, Cyber-terrorism, and Child online abuse. I*dentification, assessment and prioritization of these cyber threats are fundamental to establishing effective counter-measures and action plan framework for cybersecurity (see Figure 1), as enshrined in the National Cybersecurity Policy and Strategy.

2.3 The National Cybersecurity Strategy aggregates government collective responses towards mitigating the identified cyber threats, the risk exposure of the Nigerian cyberspace and exploiting its associated opportunities. The strategy articulates priorities, principles and approaches to understanding and managing cybersecurity risks at national level. It is a comprehensive document that provides cohesive measures and strategic

[1] *National Cybersecurity Policy 2015, Office of the National Security Adviser, Federal Government of Nigeria*
[2] *National Cybersecurity Strategy 2015, Office of the National Security Adviser, Federal Government of Nigeria*
[3] *National Security Strategy 2015, Office of the National Security Adviser, Federal Government of Nigeria*
[4] *Cybercrimes (Prohibition, Prevention), etc) Act 2015*

initiatives towards assuring security of the Cyberspace, safeguarding critical information infrastructures as well as building and nurturing a trusted cyber-community.

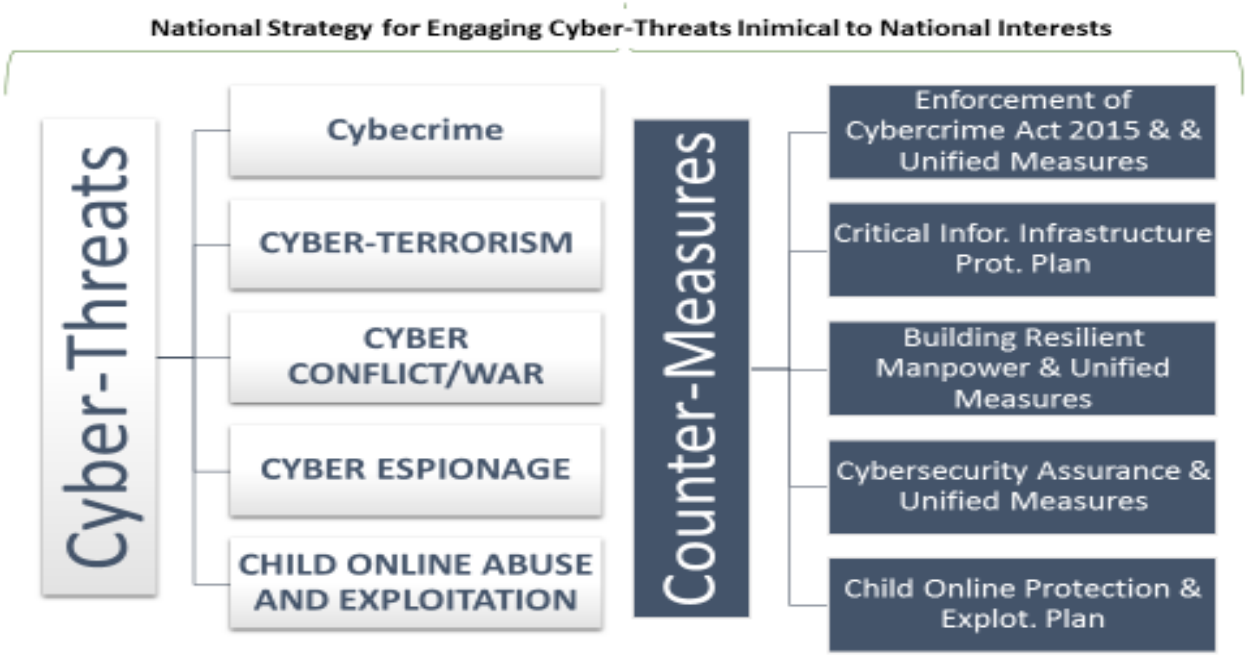


Figure 1: Extrapolation from National Cybersecurity Policy 2015

2.4 The National Cybersecurity Strategy has at its foundation, three key approaches: *multi-stakeholders engagement, public-private partnership* and *international cooperation.* The combination of these approaches are employed in the implementation of seven thematic areas that make up the National Cybersecurity Strategy, namely: legal and regulatory framework; national incident management framework; critical information infrastructure protection resilience; cybersecurity awareness and child online protection; capacity building and manpower development; cybersecurity governance as well as public-private-partnership. These thematic areas represents national priorities comprising thirty-one (31) initiatives to be implemented by relevant stakeholders in the public and private sectors, see Figure 2.

2.5 To meet Government's goal of securing Nigerian cyberspace in line with the National Cybersecurity Policy, ONSA has developed this Action Plan framework for implementing the National Cybersecurity Strategy. The Action Plan framework documents government priority, plan and direction for implementing the Strategy. It decomposes each of the seven thematic areas in the Strategy into actionable initiatives with deliverables aimed at producing tangible results. Thus, each initiative and deliverable has suggested Key Performance Indicators (KPI) with timelines to assist in measuring progress. This Action Plan is a demonstration of Government's resolve to meet cybersecurity issues head-on.

Figure 2: National Priorities and Key Thematic Areas of Engagement on Cybersecurity (Culled From National Cybersecurity Strategy).

2.6 Considering the national doctrines and principles on security, and the inter-connected nature of ICT systems and networks; multi-stakeholders synergy and inter-agency collaboration are essential for protecting the cyberspace. To this end, this draft Action Plan outlines suggested roles and expected contributions of various MDAs and key actors from the non-government sectors towards meeting the ultimate goal of making the cyberspace more secure for all Nigerians. Consequently, all stakeholders, including organised private sector are invited to key into this Action Plan for implementing

the National Cybersecurity Strategy by providing inputs and committing to fulfilling aspects of the Strategy relevant to their statutory mandates. This coordinated approach and national effort for protecting the cyberspace is crucial to enable public and private sector stakeholders effectively mitigate effects of cyber threats and make the Nigerian cyberspace safe and secure for national economic growth and development.

3.0 PROGRESS ON IMPLEMENTATION OF THE NATIONAL CYBERSECURITY STRATEGY

Some progress has been made to date with respect to the implementation of the National Cybersecurity Strategy and the Cybercrime (Prohibition, Prevention, etc) Act, 2015. Some of the activities that Government has completed or are on going are as follows:

i. **Establishment of Nigerian Computer Emergency Response Team (ngCERT)**, which serves as the Coordination Centre responsible managing for managing cyber incidents in Nigeria (Section 42 (c) of Cybercrime Act, 2015). Furthermore, ngCERT coordinates establishment and operation of sector-based Computer Security Incidents Response Teams (CSIRTS). Currently, a project is in progress to indigenously re-design and improve the capability of ngCERT's Cyber Threat Monitoring Platform, which on completion will incorporate data analytics and other artificial intelligence functionalities to enable proactive cyber incident identification and management.

ii. **Establishment of National Digital Forensic Laboratory,** which coordinate utilization of the facility by all law enforcement, security, and intelligence agencies for investigation of cybersecurity-related incidents.

iii. **Inauguration of the Cybercrime Advisory Council**, which is responsible for advising Government on measures to prevent and combat cybercrimes, threats to national cyberspace and other cybersecurity related issues.

iv. Commencement of the process for **comprehensive identification, classification and development of protection plan for critical national information infrastructure (CNII)** for all sectors of the economy. This is with a view to conducting detailed risk assessment and recommending for Presidential order to gazette the CNII. Currently, the portal to enable MDAs and private sector stakeholders to document their CNII has been deployed and the documentation process has commenced. To ensure of this project, it is essential for all stakeholders to visit the portal to document infrastructure that are critical to their operations. This is a national security assignment that is crucial to

effectively safeguard Nigerians CNII.

v. Commencement of the process for **enactment of the Data Protection and Privacy Law** for the protection of personal information of Nigerians from compromise.

vi. Implementation of **series of capacity building and training on cybersecurity for legal practitioners and Law Enforcement Agencies (LEA)** in partnership with key stakeholders.

vii. Development of this Action Plan framework for the implementation of the national cybersecurity strategy.

viii. **Developing guidelines to assist individuals and organisations report cyber incidents relating to their systems, networks and infrastructure to ngCERT**.

STRATEGY ACTION PLAN

4.0 National Cybersecurity Governance, Coordination and Assurance Mechanism.

5.0 Legal and regulatory framework

6.0 National cyber incident management framework;

7.0 Critical National Information Infrastructure (CNII) Protection and Resilience;

8.0 Cybersecurity Awareness Campaign and Child Online Protection;

9.0 Cybersecurity Capacity Building and Manpower development;

10.0 Public Private Partnership;

10.0 Assurance and Monitoring

3.0 NATIONAL CYBERSECURITY GOVERNANCE, COORDINATION AND ASSURANCE MECHANISM

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
	Implement framework for the Coordination of National Cybersecurity programs & governance **<u>OBJECTIVES</u>** To coordinate the management and implementation of national cybersecurity initiatives and all related programs as provided for in the National Cybersecurity Strategy and in line with extant laws. Monitor and Evaluate Nigerian's Cybersecurity maturity and compliance with the National Cybersecurity Strategy, Cybercrime Act, 2015 as well as guidelines, standards and other regulatory requirements. Develop comprehensive Key Performance Indicators (KPI) to measure progress and effectiveness of national efforts to combat cyber threats and counter-measures illustrated in Figure 1.	Inaugurate Cybercrime Advisory Council. Coordinate operation of the Council to function in line with provision of Sec 43 of the Cybercrime (Prohibition, Prevention, etc) Act, 2015.	Done In progress.	Establish and ensure effective functioning of all sub-committees of the Council and provide oversight functions on all national cybersecurity programs in line with provisions of the law.	*OAGF* *ONSA*
		Establish a **National Cybersecurity Coordination Centre (NCCC)** as a directorate under ONSA, to coordinate all National Cybersecurity Programs. This is in line with the provisions of the National Cybersecurity Policy & Strategy 2014. Establish a **Cybersecurity Assurance** Department under NCCC to coordinate: 1. Core Assurance Capability & Risk Assessment Program. 2. Enterprise Application Security Testing Program for critical MDAs. 3. Development of Balanced Scorecard for measuring cybersecurity maturity 4. Design a National Enterprise Security	31 December 2020 (In Progress)	Establish NCCC as a national governance and management structure to coordinate implementation of the Cybersecurity Strategy. NCCC to set up integrated operational units with processes and procedures for achieving coherent national and international engagement in cybersecurity Establish a **Cybersecurity Assurance** Department under NCCC.	ONSA to establish NCCC with organogram as shown on the *schematic at Appendix D* CAC/ONSA-NCCC & Industry stakeholders.

		Architecture Framework.			
		Establish a LEAs cybersecurity network to coordinate investigation, prosecution and enforcement of relevant provisions of the Cybercrime Act, 2015 Develop a mechanism to monitor progress of MDAs and stakeholders on implementation of the National Cybersecurity Strategy.	June 2018	Develop processes, procedures and technology as well as assign roles and responsibilities for each LEA on enforcement of key provisions of the Cybercrime Act, 2015. Establish 24/7 network of LEAs for cybercrime and assign contact persons. Establish a M&E program to monitor progress of implementing Action Plan.	ONSA

4.0 LEGAL AND REGULATORY FRAMEWORK

SN	ACTION / OBJECTIVE	DELIVERABLES	TIMELINE/ STATUS	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
4.1	**Enact a fit for purpose cybercrime legislation and national policy/strategy on cybersecurity** **OBJECTIVE** To develop and implement comprehensive cybercrime legislations, policy and strategy that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace. i. Develop Action Plan for Implement of the NCSPS. ii. Nigeria signing relevant international treaties and conventions on cybercrime and cybersecurity by Q4 2018.	Cybercrime Act, National Cybersecurity Policy and Strategy. Establish a Cybersecurity Coordination Directorate (NCCC) in ONSA.	Completed Dec 2018	Create a Cybersecurity Enforcement Directorate to facilitate enforcement of the Cybercrime Act, 2015.	CAC ONSA OAGF LEAs
		Review and update National Cybersecurity Policy and Strategy (NSCPS)	June 2019	Develop a plan, secure funding and assemble a consortium for review of the NSCPS.	CAC ONSA
		Implementation Action Plan for NSCPS	Start Jun 2017 (To complete Dec, 2018)	Complete the draft implementation action plan document. Upload document on CERT website for easy circulation among stakeholders for inputs. Incorporate inputs from stakeholders. Circulate final document to stakeholders. Develop a M&E framework for the Implementation Action Plan and assign a desk officer.	CAC ONSA MDAs/ Private Sector & NGOs
4.2	**Enact a fit for purpose legislation on data and privacy protection** **OBJECTIVE** To ensure individuals and organisations are aware of their responsibilities when handling and processing personal information. Define minimum standard and technical requirements to safeguarding personal information from compromise.	Data Protection & Privacy Act	Ongoing (To complete April 2019)	Get the National Assembly to pass into law, the bill on Data Protection & Privacy Act. Obtain Presidential accent.	NITDA / NiMC CAC ONSA OAGF

SN	ACTION / OBJECTIVE	DELIVERABLES	TIMELINE/ STATUS	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
4.3	**Develop and implement the use of Public key Infrastructure (PKI) in Nigeria** **OBJECTIVE** To establish and maintain a trustworthy digital communication and transaction environment by providing PKI and digital certificate management services with global recognition. Improve security of electronic communications and transactions.	A national PKI that is recognised globally.	Dec 2020	Establish the primary and secondary sites and Certificate Authority of national PKI	NiMC/NITDA/ CAC

5.0 NATIONAL CYBER INCIDENT MANAGEMENT FRAMEWORK

SN	ACTION / OBJECTIVE	DELIVERABLES	TIMELINE/ STATUS	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
5.1.	**Establish a national Cyber Incidents Management Framework comprising National CERT, Sectoral CSIRTs & National Digital Forensic Laboratory.** **OBJECTIVE** To provide real-time situational awareness through monitoring, evaluation and analysis of cyber-threats as well as providing timely response to cybersecurity incidents relating to the Nigerian cyberspace.	A national CERT with capability and capacity to manage and coordinate response to cyber incidents and activities of sectoral CSIRTs. Improved capability of national CERT for proactive cyber incident identification and management Establish a national digital forensic laboratory with capability for effective cyber incident handling. Develop guidelines on digital investigation and digital evidence handling.	Completed. On-going (To complete March 2019) Completed March, 2018.	National CERT with adequate visibility of Nigerian cyberspace. Incorporate trend analysis into ngCERT Cyber Threat Monitoring Platform (CMP). Develop and integrate data analytics and artificial intelligence into the platform. Improve capability of national digital forensic laboratory to conduct all components of cyber incidents handling.	ONSA/CAC ONSA/CBN/NeFF CAC/ONSA
5.2.	**Develop a National Cyber Emergency Management System (CEMS)** **OBJECTIVE** To develop and administer a National Cyber Incident response Plan outlining comprehensive cyber-threat counter measures, coordinating timely and proactive incidents management across all sectors of the economy. To facilitate periodic review of cyber threats, counter-measures, standards, guidelines and best practices for sector-based CSIRTs inline with national security imperatives.	Develop a National Cyber Incident Response Plan (NIRP) and incident management framework. Detail plan for creation of Sectorial CSIRTs. Achieve a coordinated cyber incident response across government MDAs and private sector. Develop mechanism for periodic cybersecurity briefings and publications on trend of cyber-threats and mitigation measures to all sectors of the economy	Nov, 2018	Develop a detail KPI for the NIRP. Lead key sectors to develop and implement a cyber incidents response plan. Establish mechanism for ngCERT to remotely link with sectoral CSIRTs through APIs. Ensure LEAs (with focus on NPF, EFCC, NSCDC and FMoJ) have tools required to effectively investigate and prosecute cybercrimes involving Nigeria. Classify and codify national-level cyber threats with	ONSA/NCCC/ ISPAN/ CAC/ Relevant LEAs.

SN	ACTION / OBJECTIVE	DELIVERABLES	TIMELINE/ STATUS	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
				appropriate response protocols. Develop a comprehensive distribution list for cybersecurity briefings / publications.	
5.3.	**Establish mechanism to monitor, detect and address cyber incidents on networks and systems** **OBJECTIVE** To improve capacity of LEAs, MDAs and private sector to monitor, detect, analyse and report cyber attacks.	Develop guidelines for individuals and institutions to report to ngCERT cyber attack, intrusion and interference capable of affecting other computer systems and associated networks Establish CSIRT in key LEAs, MDAs and private sector.	September 2018 June 2020	Detail guidelines for reporting cyber incident to ngCERT Coordinate creation of CSIRTs for CBN, DHQ, NIA, NPF, EFCC, NNPC, NLNG, NSCDC, NCC, NCAA and other organisations operating CNII.	ONSA-NCCC (ngCERT)
5.4.	**Strengthen measures to improve security of government networks and IT systems** **OBJECTIVE** To improve capacity of MDAs to prevent, detect, respond and counter cyber attacks against government networks and systems.	Develop and enforce security standards for the protection of government IT systems as well as online presence (websites, portals and databases). Develop and enforce security standards for the procurement of IT products and services by MDAs. Develop and enforce standard for IT Security Incidents recovery by MDAs.	June 2018 – June 2019	Develop or improve relevant standards for protection of government IT systems, online presence and procurement of IT products by MDAs. Wide circulation and public awareness on relevant standards. Establish basic security building blocks for protection of government IT systems.	NITDA NITDA ONSA-NCCC

6.0 CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII) PROTECTION AND RESILIENCE

SN	ACTION /OBJECTIVE	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
6.1.	**Identification, classification, risk assessment and develop protection plan for Critical National Information Infrastructure (CNII)** **<u>OBJECTIVES</u>** To carryout comprehensive identification, classification, risk assessment on Critical Information Infrastructure Protection (CIIP) to reduce their vulnerabilities and risk exposure to cyber incidents. Establish baseline for a regular CNII Threat Barometer & Vulnerabilities Assessment. Commence Annual National Preparedness Report on Critical Information Infrastructure security and resilience.	Comprehensive inventory of CNII. *Classify* CNII based on risk-level and criticality - document cross-sectoral dependencies of CNII. Robust protection plan for CNII. Designate CNII through a Presidential order and gazette. ***Business-Government Partnership on CIIP*** - Sensitize owners, operators and regulators of CNII, towards improving awareness on the task of identifying and protecting CNII. Annual Report on CNII Protection and Resilience.	On-going. On-going. To complete by Dec 2018	Deploy portal for documentation of CNII. Develop comprehensive inventory of Nigerian CNII based on inputs from stakeholders. Comprehensive cyber risk profile for identified CNII with mitigation strategy for the sectors identified on pp. 30 of NCSPS. Recommend list of CNII for gazette. Presidential Order and Gazette of CNII. Develop a defence-in-depth strategy for protection for each CNII with a minimum of 7 Security Layers. Sensitise owners, operators and regulators of CNII to adopt best practices in their approach to operating and managing CNII.	All stakeholders CAC/ONSA and strategic partners ONSA CAC/ONSA and strategic partners Regulators and policy makers in all sectors of the economy.
	Develop standards and guidelines for audit and protection of CNII from	Develop standards / guidelines for CNII protection.	June – Dec 2018	An approved standard for CNIIs protection (Covering	

SN	ACTION /OBJECTIVE	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
6.2.	**cyber threats.** **<u>OBJECTIVE</u>** To improve capacity of government and operators of CNII to prevent and adequately respond to cyber incidents relating to CNII through a risk-management approach (people, process and technology).	Develop guidelines /modalities for periodic auditing of CNII.		usage, access, redundancy, protection and emergency Incident Response) An approved guidelines and policy for auditing of CNIIs.	CAC, ONSA, NITDA Sector Group regulators, owners and operators of CNII NCCC/ONSA

SN	ACTION /OBJECTIVE	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
6.3.	**Enhance national readiness for protection of CNII through developing mechanism for monitoring, incident reporting, mitigation and response.** **OBJECTIVE** To enhance strategic readiness of owners/operators and regulators of CNII respond to incidents. To provide a centralised platform for information sharing and analysis of threats and vulnerabilities relating to CNII as well as mitigate risks. Implement strategies on **Prevention** and **Early Warning**, **Detection**, **Reaction**, and **Crisis Management** for security incidents relating to CNII. Ensuring CNII are less vulnerable to disruptions and interference through the following mechanisms: i. Operational mechanism towards discovering and detecting emerging threats on a timely basis. ii. Identification and correction of causes of disruption on ongoing basis. iii. Initiate alert mechanism incorporating Interdependencies of CNII to minimize impact of disruptions on the nation. iv. Establish CNII Program Modelling and Analysis (CIPMA) using super	Develop National Coordination and reporting Mechanism of cybersecurity incidents related to CNII. Develop National CII Protection and Incident Response Plan covering strategies for prevention and early warning, detection, reaction and crisis management. Develop sector-specific plan for each sector listed on Page 30 of the National Cybersecurity Strategy. Establish CNII Trust Information Sharing Network (TISN) / Forum involving Infrastructure owners, operators and regulators to achieve cross-sectorial dependencies and management.	Jan – June 2019	CNII incident reporting mitigation and response strategy widely circulated to relevant stakeholders ngCERT to establish direct API access to monitor all CNIIs. Establish CNII Trust Information Sharing Network (TISN) / Forum.	ONSA/NCCC /Sector Group regulators, owners and operators of CNII.

SN	ACTION /OBJECTIVE	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
	computers to evaluate consequences and develop mitigation measures for different disasters and threats (human and natural) situations.				

7.0 NATIONAL AWARENESS ON CYBERSECURITY, INTERNET SAFETY AND CHILD ONLINE PROTECTION

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
7.1	Improve national awareness on cybersecurity/internet safety across all segment of Nigerian society through targeted awareness campaign/advocacy **OBJECTIVE** To provide Nigerians with information to protect themselves, families and organisations online through raising awareness of the Cybercrime Act, 2015, trend of evolving cyber threats with mitigation measures.	Conduct baseline public opinion poll to determine awareness level and attitude of Nigerians on cybersecurity. Assessment of Nigerian dominant cyber threats to establish baseline threat landscape, trend and methods. Use established baseline to develop and implement plan for cybersecurity awareness campaign through multi-stakeholders engagement covering workshops, seminars, advertising, web, social media and special events across the six geopolitical zones, MDAs and industries. Distribute to all stakeholders, copies of the Cybercrime (Prohibition, Prevention, etc) Act, 2015, National Cybersecurity Strategy and its implementation Action Plan.	March 2018 Dec 2018 March 2019	Develop and implement a comprehensive plan for cybersecurity awareness campaign for different segments of Nigerian society: legislature, policy makers, civil servants, university lecturers and students, LEAs and general public using all available communication channels. Secure agreement with MDAs and private organisations to sponsor cybersecurity awareness programme. Identify a minimum of 7 change agents and cybersecurity ambassadors across the country. 50% of the Nigerian Public fully aware of the relevance of the Cybercrime Act, 2015 in improving national cybersecurity posture.	ONSA/NCCC/NITDA /NOA/Min of Info/NeFF CAC, ONSA-NCCC

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
7.2	**Create and implement mechanism for child online protection** **OBJECTIVE** To institutionalise a framework to reduce vulnerability and ensure safety of children interaction online.	Establishment of a Unit under NCCC to handle matters relating to Child Online Abuse and Exploitation (COAEP) within the scope of National Cybersecurity Policy. Develop and implement plan for reducing vulnerability of children online through the following initiatives: **Initiative 1**: Develop plan for improving awareness among children on **Cyber Safety.** **Initiative 2**: Establish mechanism involving ngCERT/ISPs for reporting and removing or blocking access to illegal content of child sexual abuse found on the internet. **Initiative 3**: Build capacity and provide forensic tools for LEAs to investigate internet related crimes against children and young people and maintain a register of such offenders.	Sep 2018 – Sep 2020	Develop school-based awareness programmes on cyber safety for primary and secondary schools. Establish and circulate a working mechanism for reporting illegal content of child sexual abuse found on the internet.	ONSA-NCCC /NCC/ NiRA/NAPTIP/Ministry of Education

8.0 NATIONAL CYBERSECURITY SKILLS AND MANPOWER DEVELOPMENT

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
8.1	**Build capacity of the judiciary and Law Enforcement for cybercrime investigation, prosecution and adjudication** **OBJECTIVE** To improve skills and competence of judicial officers and law enforcement agencies (LEAs) in handling cybercrime cases.	Establish baseline number of trained officers in the judiciary and LEAs with skills in investigation / prosecutions and adjudication of cybercrime cases. Increase the number of skilled personnel by 50%.	On-going (To be completed June 2020)	Get inputs from OAGF and LEAs. Secure funding/partnership for training. Develop and implement the training plan. M&E progress.	CAC OAGF /ONSA
8.2	**Establish institutional framework for cybersecurity skills and manpower development** **OBJECTIVE** To generate highly skilled manpower in Cybersecurity with professional competence based on international good practice.	Established Nigerian Institute off Cybersecurity. Developed roadmap for professional training and capacity building in Cybersecurity. Establish mechanism for accreditation of Cybersecurity courses/curriculum in Nigerian Universities. Build capacity of IT staff in MDAs in special areas of cybersecurity, including auditing, risk evaluation & management, forensic investigation and protection of CNII. Develop specialise training on building capability of CERTS and CSIRTs.	June 2018 – June 2020	Unified scheme for national certification training in cybersecurity based on international approved standards. International recognition for Nigerian Institute of Cybersecurity. Develop capacity of graduates of Computer Science/Cybersceurity from Nigerian Universities to cope with the dynamic nature of global cybersecurity threats. Increase by 50% the number of IT personnel in MDAs with	ONSA/ CAC NCCC CAC/Ministry of Education/NUC/FMoCT NITDA / FMoCT

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
				specialist skills in cybersecurity.	
8.3	**Build a national framework for promoting cybersecurity research, innovation & local content development** **OBJECTIVE** To create a roadmap for empowering cybersecurity professionals to develop local ICT contents and innovation	**Establish a Cybersecurity Centre of Excellence in one university in each geo-political zone in Nigeria** Build a team of experts with capacity to carry out research, development and training in key areas of cybersecurity.	June 2019 – June 2021	An R&D Endowment Intervention in selected Nigerian Universities to support setting up of Cybersecurity Centre of Excellence Support Indigenous ICT Institute on software and hardware development. Sponsor innovative research outputs in various aspects of Cybersecurity. Selected Centres of Excellence to be involved in CIPMA program.	ONSA-NCCC, NITDA, NCC NUC/NBTE/ NeFF/PTDF

9.0 PUBLIC PRIVATE PARTNERSHIP

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
9.1	**Develop a Public-Private Partnership Programs for Implementing National Cybersecurity Strategy** **<u>OBJECTIVES</u>** To build national capabilities against cyber threats through collaboration among public-private sector partners and multi-stakeholder engagement. To engage States and Local Governments on cybersecurity, seek their active involvement in securing computer systems and networks and other facilities within their jurisdiction.	Establish Public-Private Partnership (PPP) Technical Working Group (NTWG) on cybersecurity. Create private sector and state government led PPP initiatives on improving cybersecurity at states and local government level.	June 2018–June 2020	Establish NTWG Established private-sector-based CSIRTS at various organs based on PPP Coordinate timely response to national/ international cybersecurity challenges. A minimum of one CSIRT team in each geopolitical zone.	CAC & ONSA-NCCC NCCC/NITDA
9.2	**Develop public-private information sharing arrangement and protocol** **<u>OBJECTIVES</u>** To build a trusted platform for strategic information sharing between government and private sector to proactively identify, monitor and respond to cyber threats.	Develop and implement guidelines and policies for information sharing. Establish sector specific plans of regulating agencies on information sharing based on threats and vulnerabilities of the sectors.	Jan 2018–Jan 2020	Designated functional platform for information sharing of the public and private sectors. Regular or periodic feedbacks from regulating agencies and access to information on threats and vulnerabilities of private sector.	NITDA Regulating Agencies of Various Sectors

SN	ACTION PLAN	DELIVERABLES	TIMELINE	KPI	POLICY DRIVERS
(a)	(b)	(c)	(d)	(e)	(f)
9.3	**PPP arrangement for Protection of Critical Information Infrastructure (CII), computer and network assets with impact on the economy and security.** **<u>OBJECTIVES</u>** To engage owners and operators of Nigeria's critical infrastructure and key network assets including the private sector on technological innovations, critical resources and technical standards required for their seamless operation.	Establish a CNII Information Sharing and Analysis Centre (ISAC) for government and operators of CII. Formation of National Cybersecurity Forum comprising ngCERT, CSIRTS, private companies and international partners. Establish critical information infrastructure program modelling and Analysis (CIPMA). Establish Nigerian Institute of Cybersecurity.	June 2018 –June 2020	Establish CNII ISAC Roadmap and implementation action plan on activities of National Cybersecurity Forum	ONSA/NITDA ONSA/NITDA ONSA/NITDA/coordinating Ministries/regulators

APPENDIX A

LIST OF ABBREVIATIONS

API	APPLICATION PROGRAMME INTERFACE
CAC	CYBERSECURITY ADVISORY COUNCIL
CBN	CENTRAL BANK OF NIGERIA
CEMS	CYBER EMERGENCY MONITORING SYSTEM
CERT	COMPUTER EMERGENCY RESPONSE TEAM
CIA	CONFIDENTIALITY, INTEGRITY, AVAILABILITY
CIIMP	CRITICAL INFORMATION INFRASTRUCTURE MEASURING PROGRAMME
CIIP	CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
CIPMA	CNII PROGRAM MODELLING AND ANALYSIS
CNII	CRITICAL NATIONAL INFORMATION INFRASTRUCTURE
CNIIP	CRITICAL NATIONAL INFORMATION INFRASTRUCTURE PROTECTION PLAN
COAEP	CHILD ONLINE ABUSE AND EXPLOITATION
CSIRT	COMPUTER SECURITY INCIDENCE RESPONSE TEAM
FMoCT	FEDERAL MINISTRY OF COMMUNICATION TECHNOLOGY
ICT	INFORMATION AND COMMUNICATIONS TECHNOLOGY
ISAC	INFORMATION SHARING AND ANALYSIS CENTRE
ISP	INTERNET SERVICE PROVIDER

NAPTIP	NATIONAL AGENCY FOR THE PROHIBITION OF TRAFFICKING IN PERSONS
NBTE	NATIONAL BOARD FOR TEACHNICAL EDUCATION
NCC	NIGERIAN COMMUNICATION COMMISSION
NCSS	NATIONAL CYBERSECURITY STRATEGY
NDFL	NATIONAL DIGITAL FORENSIC LABORATORY
NeFF	NIGERIAN EFRAUD FORUM
NgCERT	NIGERIAN COMPUTER EMERGENCY RESPONSE TEAM
NIMC	NATIONAL IDENTITY MANAGEMENT COMMISSION
NIRP	NATIONAL INCIDENCE RESPONSE PLAN
NITDA	NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY
NOA	NATIONAL ORIENTATION AGENCY
NTWG	NATIONAL TECHNICAL WORKING GROUP
NUC	NATIONAL UNIVERSITIES COMMISSION
OAGF	OFFICE OF THE ATTORNEY GENERAL OF THE FEDERATION
ONSA	OFFICE OF THE NATIONAL SECURITY ADVISER
NSCPS	NATIONAL CYBERSECURITY POLICY AND STRATEGY
POC	POINT OF CONTACT
PPP	PUBLIC PRIVATE PARTNERSHIP
PTDF	PETROLEUM TECHNOLOGY DEVELOPMENT FUND

S-CERT	SECTORAL COMPUTER EMERGENCY RESPONSE TEAM
SRP	STRATEGIC READINESS PLAN
TISN	TRUST INFORMATION SHARING NETWORK

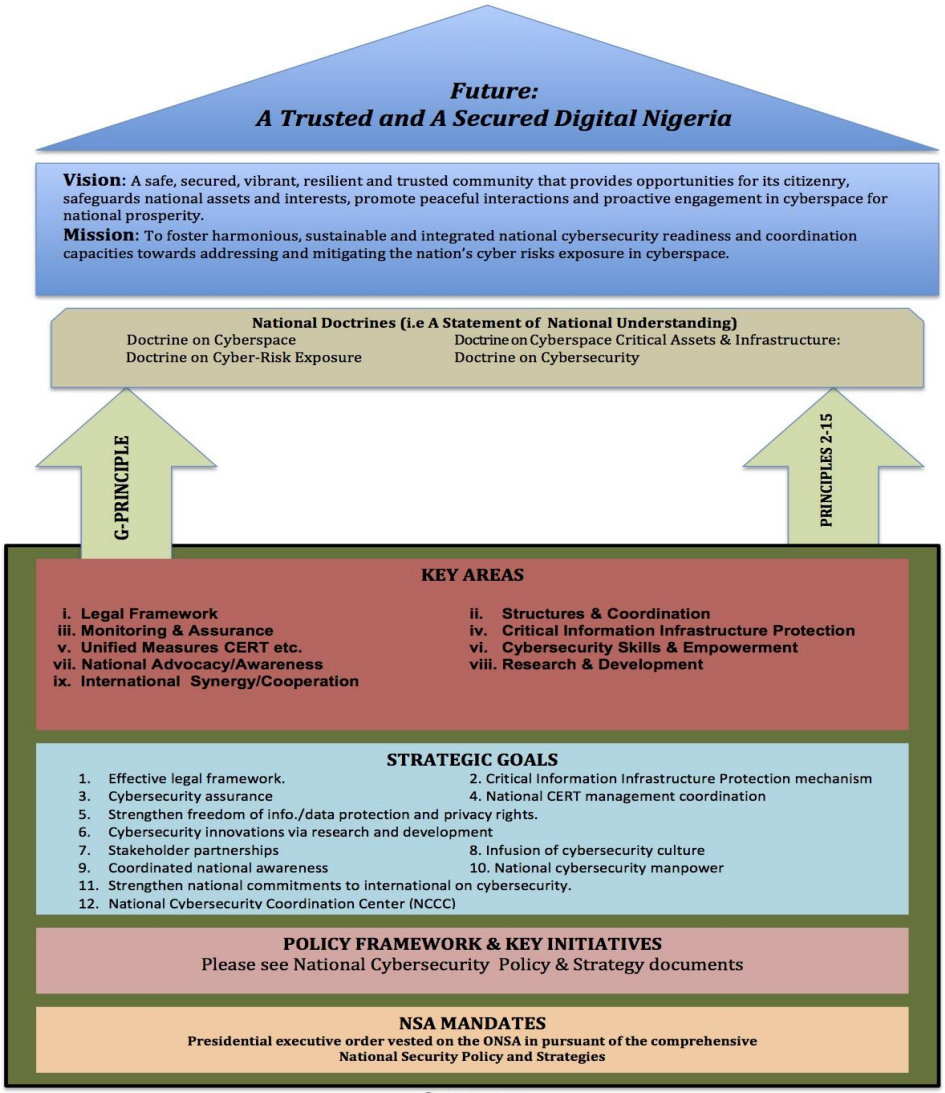
APPENDIX B

Definitions

Cookies	Cookies are small text files, given Identity tags that are stored on your computer's browser directory or program data subfolders.
Cybercrime	Cybercrime is criminal activity undertaken using computers and the Internet.
Cyberspace	The electronic medium of computer networks, in which online communication takes place
Cybersecurity	Cyber security includes information and technical security applied to hardware, software and systems that make up networks
Cyberthreat	The possibility of a malicious attempt to damage or disrupt a computer network or system
Cyber-Terrorism	The intentional use of computer, networks, and public internet to cause destruction and harm
Data Protection	legal obligations around control over processing ,access and use of personally identifiable information
Data Retention	Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements
Economic espionage	A form of espionage conducted for commercial purposes instead of purely national security
Hactivism	The use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics. It is carried out under the premise that proper use of technology can produce results similar to those of conventional acts of protest, activism, and civil disobedience.
Lawful Interception	Obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence.
Military espionage	Spying on potential or actual enemies primarily for military purposes
Privacy	The right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organisational information is to be revealed
Vulnerability	A weakness which allows an attacker to reduce a system's information assurance

APPENDIX C

OVERVIEW OF THE NATIONAL CYBERSECURITY STRATEGIC ROADMAP



APPENDIX D

SCHEMATIC OF NCCC COORDINATION FRAMEWORK