FEDERAL REPUBLIC OF NIGERIA

NATIONAL CYBERSECURITY POLICY AND STRATEGY 2021

Summary

VISION

A safe and secure digital community that provides opportunities for its citizenry and promotes peaceful and proactive engagements in cyberspace for enhanced national prosperity

MISSION

To foster a trusted cyber environment that optimises Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure

The National Cybersecurity Policy and Strategy 2021 is a purposeful and living document which outlines the roadmap for realisation of our cybersecurity Vision and Mission. The document is a confluence of ends, ways and means which articulates the efforts of all stakeholders and emplaces our National Cybersecurity Programme on 8 critical pillars

8 Pillars to form the support for our national cybersecurity program

- Strengthening Cybersecurity Governance and Coordination
- Fostering Protection of Critical National Information Infrastructure
- Enhancing Cybersecurity Incident Management
- Strengthening Legal and Regulatory Framework
- Enhancing Cyber Defence Capability
- Promoting a Thriving Digital Economy
- Assurance Monitoring and Evaluation
- Enhancing International Cooperation

In line with the provisions of Section 41 of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 which empowers the Office of the National Security Adviser to be the coordinating body for national cybersecurity, the National Cybersecurity Coordination Centre (NCCC) is entrusted with the responsibility of aligning and harmonising the efforts of all stakeholders towards the delivery of our National Cybersecurity Programme

NCCC

To deliver the objectives of our National Cybersecurity Programme, we have an Implementation Plan that is our roadmap for driving success, measuring progress and transforming our prescribed strategic actions into reality. The key actions are:

Strengthening Cybersecurity Governance and Coordination

- Establishment of National Cybersecurity Coordination Centre
- Driving Awareness of Cybersecurity Stakeholders' Responsibilities

Fostering Protection of Critical National Information Infrastructure (CNII)

- Comprehensive approach to CNII Protection and Resilience
- Identifying and Coordinating CNII Sectors and Dependencies
- Developing CNII Protection Plan

Enhancing Cybersecurity Incident Management

- Coordination of national cybersecurity incident management
- Establishment of Sectoral CSIRTs
- National Crisis Response Plan

Strengthening Legal and Regulatory Framework

- Review and harmonisation of existing legal framework on cybersecurity (including e-business and online consumer protection).
- Internet Safety and Protection of Children and Gender Rights Online
- Developing the capacity of the judiciary and law enforcement to address cybercrime

Enhancing Cyber Defence Capability

- Administering the activities of the cyber establishments of the armed forces and law enforcement agencies
- Development of a cyber defence plan for Nigeria
- Training of the armed forces to protect the Nigerian cyberspace

Promoting a Thriving Digital Economy

- Promoting the use of the cyberspace to drive Nigeria's digital economy
- Building trust and confidence in a safe and resilient Nigerian cyberspace
- Promoting an indigenous cyber workforce
- Driving a high level of awareness on cybersecurity

Assurance Monitoring and Evaluation

- Deployment of robust and high-quality cybersecurity technology to safeguard our cyberspace
- Strengthening Standards and Good Practices in Public and Private Sectors
- Deployment of Quality Controls and Security Processes

Enhancing International Cooperation

- Alignment of efforts of domestic cybersecurity stakeholders within Nigeria to enhance international engagement
- Strengthening cybersecurity influence on the regional stage
- Providing support for international mechanisms that promote cybersecurity

As the country sets out to implement the strategic measures and unlock national potentials for ensuring progressive use of the nation's cyberspace, all stakeholders have a mandate to make conscious effort to balance the security, social and economic imperatives of cyberspace with the cybersecurity needs of government, industry, academia and the international community.