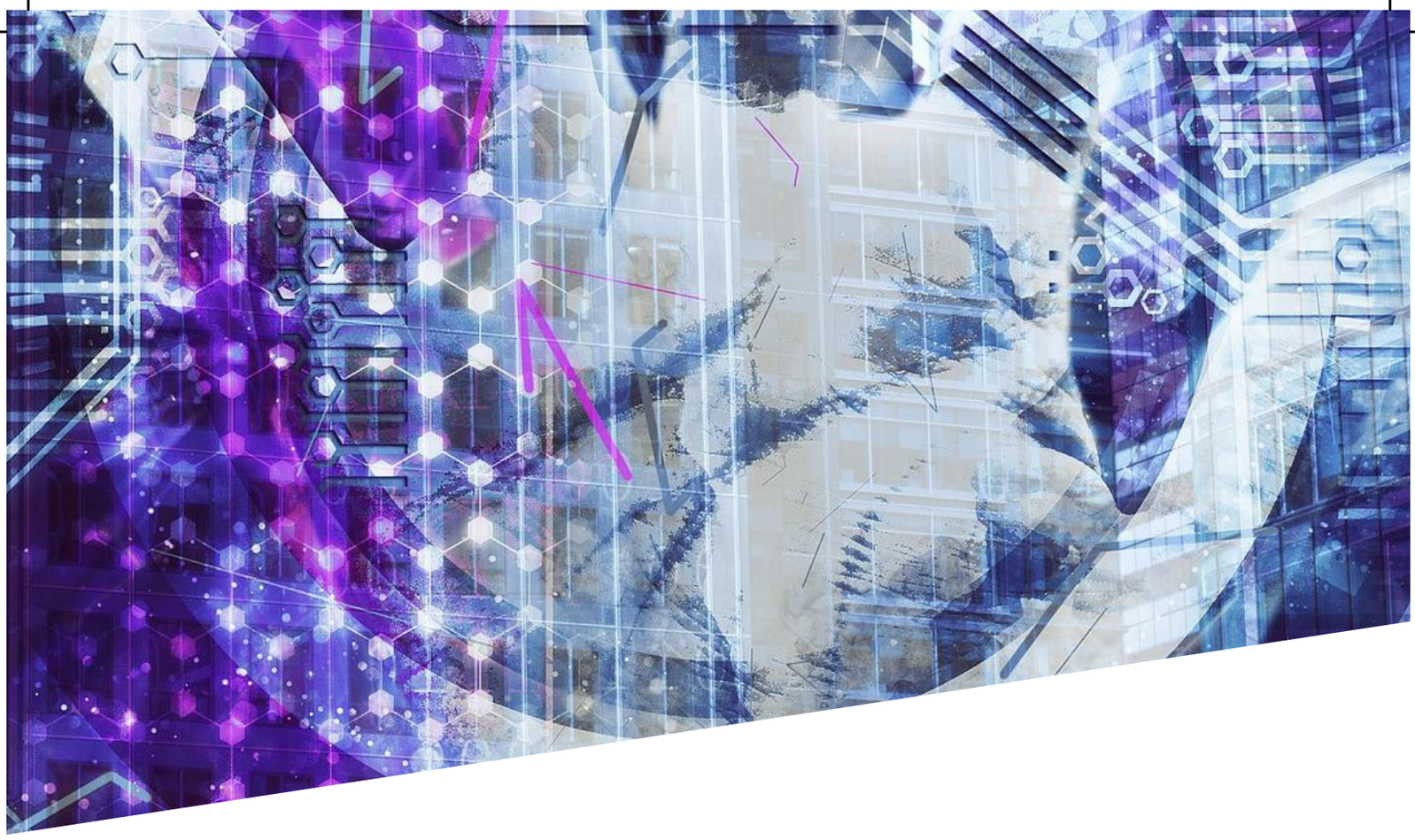


NATIONAL CYBERSECURITY POLICY & STRATEGY, 2021

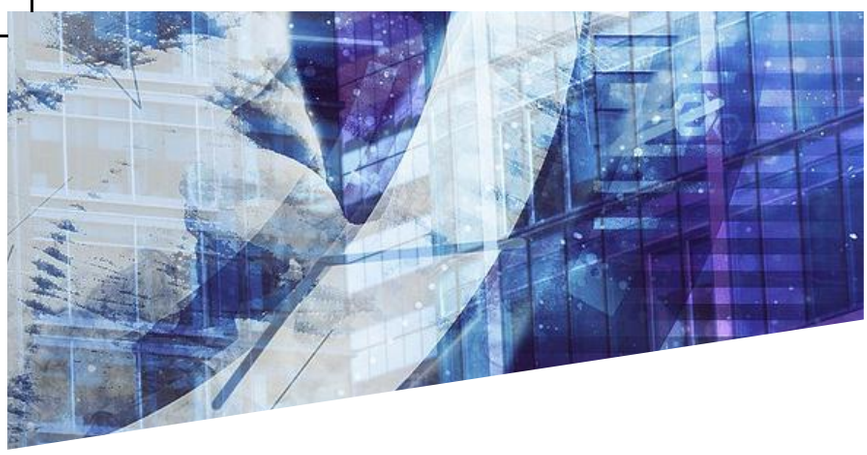
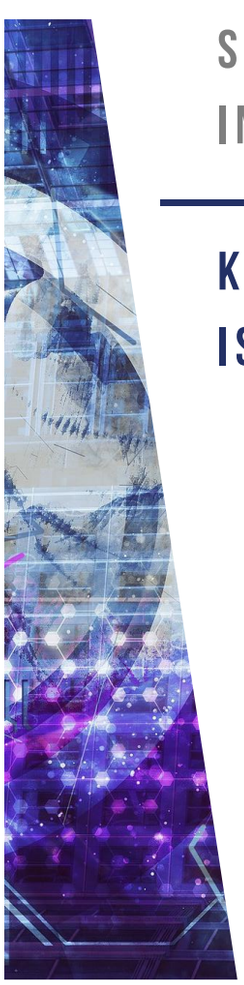


TABLE OF CONTENTS

01 INTRODUCTION TO THE POLICY

TITLE	National Electronic Health Bill, 2019
REFERENECE NO:	API10/NCPS/001/0421
DOCUMENT TYPE:	Federal Policy
RELEVANT SECTORS / INDUSTRY	• Information and Communication Technology • Digital Economy • Entrepreneurship • Financial Technology • Education
KEY ISSUES	• Establishment of National Cybersecurity Coordination Centre (NCCC) and National Cybersecurity Training Institute • Information Sharing • Licensing of Cybersecurity Professionals and Centres • Funding • Establishment of Sectoral Computer Security Incident Response Team • Records for the Documentation and Archiving of Threats and Vulnerabilities • Register for Convicted Online, Child and Gender Abusers/offenders



02 OVERVIEW OF THE POLICY

The National Cybersecurity Policy and Strategy 2021 policy document draws its foundation from the 2015 National Cybersecurity Policy and Strategy and is expected to address Nigeria's cybersecurity challenges, enhance digital competitiveness, improve indigenous technology development and safeguard Nigeria's Critical National Information Infrastructure.

This policy document is expected to foster cooperation with Nigerian international allies in security and economic development as well as ensure the protection of Nigeria’s cyberspace from cyber-attacks, online fraud, and other related illicit activities such as fake news and hate speech.

The policy document is expected to serve as a strategic roadmap for all stakeholders, including Ministries, Departments and Agencies of Government, the private sector, academia, professional bodies and global partners to drive Nigeria's cybersecurity objectives.

This policy document is expected to foster cooperation with Nigerian international allies in security and economic development as well as ensure the protection of Nigeria’s cyberspace from cyber-attacks, online fraud, and other related illicit activities such as fake news and hate speech.
objectives.

The policy document is expected to serve as a strategic roadmap for all stakeholders, including Ministries, Departments and Agencies of Government, the private sector, academia, professional bodies and global partners to drive Nigeria's cybersecurity objectives.

03 CRITICAL INTERESTS

FOR THE BILL

- Office of the National Security Adviser
- Space Administration
- Federal Ministry of Communications and Digital Economy
- Federal Ministry of Justice
- National Information Technology Development Agency
- Federal Ministry of Industry and Trade
- Ministry of Defense
- Nigerian Communication Commission
- National Office for Technology Acquisition and Promotion
- Federal Competition and Consumer Protection Commission
- Nigeria Security and Law Enforcement Agencies
- Federal Ministry of Science and Technology
- National Universities Commission

AGAINST THE BILL

- Nil

MODIFICATION OF THE BILL

- Nil

INDIFFERENT

- Nil

04 IMPLICATIONS

Establishment of a National Cybersecurity Coordination Centre (NCCC)

The policy and strategy document provides for the establishment of the NCCC. The NCCC is to be led by a national coordinator and will serve as the focal point for cybersecurity in Nigeria both locally and internationally.

Mandatory Registration of Critical National Information Infrastructure

Owners and operators of Critical National Information Infrastructure (CNII) will be expected to register their infrastructure with the government for joint development and infrastructure protection. The document provides no details for the process of joint security and protection.

Mandatory Information Sharing

Owners and Operators of CNII will be mandated to share information on threats, vulnerabilities, strategies and solutions to mitigate the risk of CNII between them and the NCCC. This is to be done through a Trusted Information Sharing Network forum established under NCCC. This forum will consist of owners and operators of CNII and stakeholders from government departments and agencies. The NgCert, under the NCCC, shall develop an Auto Cyber-Indicator Sharing (ACIS) system to facilitate real-time incident information exchange on the cybersecurity-related incident between owners and operators of CNII.

Mandatory Periodic Audits

Private owners and operators are required to conduct periodic audits and participate in the National Critical Information Infrastructure Measurable Programme organized by NCCC for the progress monitoring and evaluation of CNII risk levels.

Guidelines and Standards

NCCC may issue guidelines and standards for the CNII owners and operators towards safeguarding their systems and networks. It is however doubtful that this power can be delegated to the NCCC. The NCCC, in collaboration with NITDA, may issue guidelines and standards for the procurement, development, utilisation and deployment of cybersecurity hardware and software technology systems.

Mandatory Cyber Security Crisis Response and Exercise Drills

CNII owners and operators will be obligated to participate in cybersecurity crisis response exercise and drills in preparedness for responding to cyber incidents and threats. The processes for these drills are not stipulated in the document.

Encourage the Use and Adoption of Local Content

NCCC shall collaborate with relevant stakeholders to create cybersecurity technology incubation platforms, innovation centres, and laboratories that shall drive initiative and provide support and incentives for projects focusing on the indigenous cybersecurity technology market in Nigeria.

Centralized Licensing and Registration

NCCC will be the sole body to license cybersecurity professionals in Nigeria. Cybersecurity training centres and institutions, cyber cafes and security service providers will be required to register and license with NCCC before they can operate in Nigeria.

Financial Incentives

Tax holidays, innovation grants and pioneer status shall be granted for indigenous innovation and development of cybersecurity technologies and cybersecurity research.

For access to the full report,
please send "Subscribe" to:
subscriptions@apiintelligence.org