

The Federal Government Has Officially signed the Designation and Protection of Critical National Information Infrastructure Order 2024

The Federal Government has issued a new order aimed at enhancing the security of Nigeria's Information and Communications Technology (ICT) systems. This order is titled the Designation and Protection of Critical National Information Infrastructure Order 2024. The Order was recently published in an official gazette signed by President Bola Tinubu.[1]

This Order also serves as an extension of the Cybercrimes (Prohibition, Prevention etc.) Amendment Act 2024, specifically addressing Parts II & III of the Cybercrimes Amendment Act 2024.[2]

Over the years, stakeholders in the Nigerian ICT sector have urged the government to designate telecom infrastructure as a critical national asset to address the ongoing attacks on this infrastructure across the country. For instance, in 2023, it was reported that MTN Nigeria suffered over 6,000 incidents of fiber cable damage.[3] Also, in June 2024, as part of a nationwide industrial action against the Federal Government's ₦60,000 minimum wage proposal, civil servants affiliated with the Nigerian Labour Congress shut down the national grid.[4]

---

1 The publication of the Designation and Protection of Critical National Information Infrastructure Order 2024 in the official gazette has garnered notable attention across media platforms. News outlets have highlighted its significance in fortifying national cybersecurity and safeguarding critical sectors. This development is set to be a focal point of coverage following President Bola Tinubu's endorsement, which underscores the government's commitment to protecting national information infrastructure.

2 Section 3 of the Cybercrimes Amendment Act 2024 empowers the President of the Federal Republic of Nigeria, upon recommendation of the National Security Adviser, to publish an order in the Federal Gazette designating certain computer systems or networks as Critical National Information Infrastructure (CNII).
Also, Section 5 of the Cybercrimes Amendment Act 2024, provides for the offences and penalties related to violations against Critical National Information Infrastructure (CNII).

3 Punch, "Telcos Record ₦27bn Loss from Damaged Fiber Cables" available at https://punchng.com/telcos-record-n27bn-loss-from-damaged-fibre-cables/ accessed 12th September 2024.

4 CNN, "Nigeria Plunged Into Darkness as Union Workers Shut Down National Grid in Minimum Wage Protest" available at https://edition.cnn.com/2024/06/03/africa/nigerian-workers-declare-nationwide-strike-intl/index.html accessed 12th September 2024.

Therefore, the establishment of this Order is to develop cohesive measures and strategies for securing and protecting these critical infrastructures and ensuring their ongoing availability and deployment for the benefit of the nation.

The target of this Order is to protect and ensure the effective functioning of ICT systems, networks, and infrastructure, which are critical to driving national imperatives, economic development, national security and defence, public health and safety, and government operations.[5] This Order also stipulates that anyone who attacks any infrastructure listed in the gazette commits an offence and is liable to prosecution.

This Order represents a significant step in Nigeria's commitment to securing critical digital infrastructure, supporting national security, economic growth, and public safety.

The Key objectives of the Designation and Protection of Critical National Information Infrastructure Order 2024 include:

1. **Designation of Critical National Information Infrastructure (CNII) in various sectors in the Nigerian Economy**: The Order officially designates ICT systems in various sectors of the Nigerian economy as CNII. These sectors include power and energy, water, communications, finance, health, defense and security, transportation, and more.[6] This reflects the critical role these sectors play in national security and economic development.
2. **Holistic Protection Strategy**: A Critical National Information Infrastructure Protection Plan (CNIIPP) will be developed, setting minimum standards, procedures, and security measures to safeguard CNII.[7] The CNIIPP is a comprehensive approach to secure and protect Critical National Information Infrastructure. By ensuring their continued operation, it aims to prevent damage or disruption to critical ICT systems and networks.
3. **Trusted Information Sharing Network (TISN)**: To foster collaboration, the Order establishes a multidisciplinary framework known as Trusted Information Sharing Network (TISN). This network will include CNII owners, operators, relevant government ministries, and private sector entities. Together, they will work to assess

---

5 Paragraph 1 of the Designation and Protection of Critical National Information Infrastructure Order 2024.

6 Paragraph 2(2) of the Designation and Protection of Critical National Information Infrastructure Order 2024.

7 Paragraph 3 of the Designation and Protection of Critical National Information Infrastructure Order 2024.

and mitigate risks, share best practices, and build capacity for strengthening CNII resilience.[8]

4. **General Oversight**: The Order empowers the Office of the National Security Adviser (ONSA) to oversee audit compliance, and any guideline or rule made pursuant to this order.[9]

5. **Offences and Penalties**: The Order outlines penalties for unauthorized access, tampering, or interference with CNII. Individuals who engage in fraudulent acts against CNII systems will face prosecution and penalties as prescribed by law, ensuring strict enforcement of protective measures.[10]

With the increasing reliance on digital infrastructure for essential services in Nigeria, the Designation and Protection of Critical National Information Infrastructure Order 2024, provides a robust legal framework to ensure the continued security and resilience of Nigeria's critical infrastructure. The security and protection of these Critical National Information Infrastructure (CNII) will help improve the quality of telecoms services which has very often been affected by disruption and intentional damage.

Stakeholders in the sectors listed in the order are encouraged to take proactive steps to comply with the Order and contribute to safeguarding national security.

Access an electronic copy of the Designation and Protection of Critical National Information Infrastructure Order 2024 here to read up on the Order.

---

8 Paragraph 4 of the Designation and Protection of Critical National Information Infrastructure Order 2024.

9 Paragraph 6 of the Designation and Protection of Critical National Information Infrastructure Order 2024.

10 Paragraph 7 of the Designation and Protection of Critical National Information Infrastructure Order 2024.