STRENGTHENING NATIONAL SECURITY WITH RIGHTS-BASED GOVERNANCE:

Public Interest Concerns on the Designation and Protection of Critical National Information Infrastructure (CNII) Order, 2024

Policy Brief **September, 2025**

Table of Contents

EXECUTIVE SUMMARY

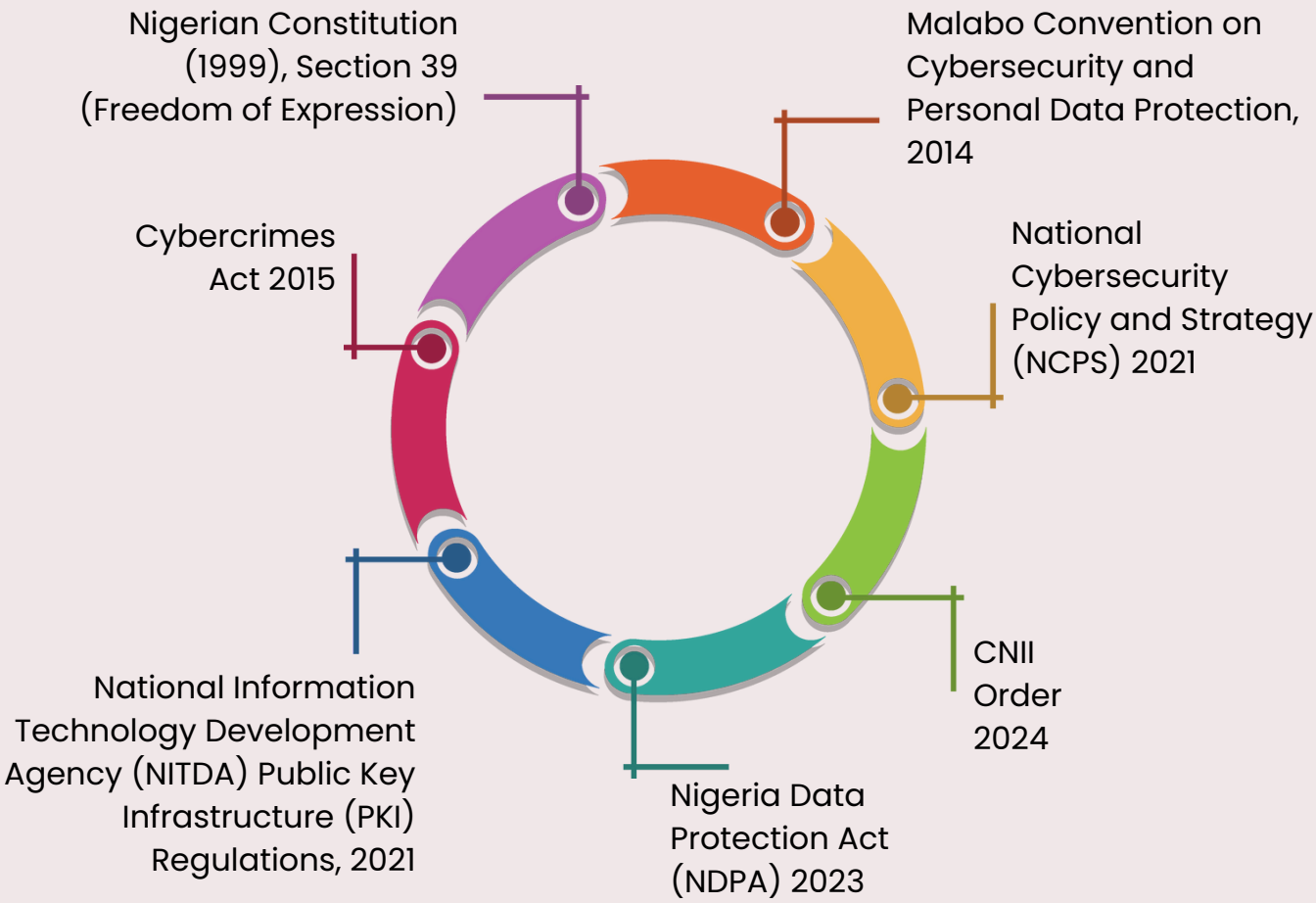
The Designation and Protection of Critical National Information Infrastructure (CNII) Order, 2024, expands the scope of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, by introducing stricter provisions and enforcement powers relating to digital public infrastructure (DPI). While these measures aim to enhance cybersecurity, their implementation raises significant public interest concerns, particularly regarding legal overreach, opaque governance, and risks to fundamental rights.

The urgency and significance of this debate are especially clear in an era where elections are increasingly digital, citizens depend on national digital IDs like the National Identification Number (NIN) to transact online, and where economic activities hinge on trusted online systems. In Nigeria, cybersecurity governance is a fundamental question of democratic accountability, digital rights, and the preservation of public trust in digital governance.

This brief presents the views of the Data and Digital Rights Coalition, coordinated by Accountability Lab (AL) Nigeria, on the risks posed by the CNII Order in its current form. We recommend a recalibration of its enforcement framework to ensure alignment with Nigeria's constitution, international human rights norms, and national data protection act. Our recommendations include clearer legal definitions, non-state actor inclusion in oversight, and safeguards for ethical disclosures.

BACKGROUND

The CNII Order, issued under the Cybercrimes Act 2015, empowers the Office of the National Security Adviser (ONSA) to designate and protect infrastructure critical to national security. The Order criminalizes unauthorized access, tampering, or interference with CNII and invokes penalties in line with Part 3 of the Cybercrimes Act. The relevant laws and frameworks include:



Despite these frameworks, the implementation of CNII protections lacks clarity and appears to conflict with fundamental human rights and Nigeria's data protection commitments.

PUBLIC INTEREST CONCERNS

Vagueness and Overreach of Legal Provisions:

Section 10 of the Cybercrimes Act and Paragraph 7 of the CNII Order criminalize broadly defined acts like tampering or unauthorized access, without adequate public interest protections. This vagueness risks the criminalization of ethical disclosures by whistleblowers, researchers, and journalists. Nigeria has repeatedly used ambiguities in the Cybercrimes Act, particularly Section 24, to arrest journalists and activists for online speech. CSOs have documented instances where individuals faced prosecution for merely voicing legitimate criticism of public officials. Despite the 2024 amendment, which was intended to narrow the scope of cyberstalking offences, enforcement patterns remain troubling. In one case involving Strategic Lawsuits Against Public Participation (SLAPP), four individuals were charged over allegedly defamatory publications about the Chief Executive Officer (CEO) of a major bank. This trend reflects concerns captured in the Freedom on the Net 2024 report, which ranked Nigeria as Partly Free, with a score of 59 out of 100, citing a sustained decline in online freedom and growing legal threats to expression. A 2023 breach of the National Identity Number (NIN) database revealed weak CNII protections, with no coordinated institutional accountability despite significant public interest implications. The lack of harmonization between CNII enforcement and the NDPA reflects a systemic gap that undermines both trust and resilience;

Lack of Transparency in CNII Designation:

The CNII designation process is unclear, lacking a publicly accessible list or criteria for determining what qualifies as critical infrastructure. This situation limits institutional accountability and increases the risk of politicized or arbitrary enforcement, especially during elections or civic protests. As of 2024, no registry exists to guide public or institutional awareness of CNII obligations. This contradicts global best practices and impedes trust-building between regulators and stakeholders;

Disproportionate Penalties without Public Interest Safeguards:

The CNII Order imposes harsh penalties, fines, and imprisonment for violations, even in cases of internal errors, whistleblowing, or investigative journalism. In August 2024, PIDOM (Isaac Bristol Tamunobifiri) was arrested for exposing security flaws and leaking official documents. His arrest raised concerns about the risks faced by whistleblowers in Nigeria. In May 2024, investigative journalist Daniel Ojukwu was detained after exposing ₦147.1 million in public procurement irregularities. These cases illustrate how fragmented legal protections across the Cybercrimes Act, the ICPC and the Federal Ministry of Finance whistleblower

policy create an unsettling effect on public interest reporting, which continue to undermine efforts to strengthen transparency and secure critical systems;

Regulatory Fragmentation:

Although the Cybercrimes Act was amended in 2024, its historical misuse to curb online expression, such as the 2021 Twitter ban, signals the dangers of loosely defined cyber laws. The CNII governance lacks alignment with Nigeria's broader cybersecurity and data protection frameworks. While Section 21(1) of the Cybercrimes Act mandates immediate reporting of cyber incidents to the National Computer Emergency Response Team (CERT), through sectoral CERTs or security operations centres (SOCs), and Section 40(2) of the NDPA requires data breach notifications to the Nigeria Data Protection Commission (NDPC) within 72 hours with steep penalties for non-compliance, there is no clear guidance under the CNII Order on how designated CNII operators or certification authorities should fulfil these obligations. NITDA's PKI Regulations require accredited certification authorities to maintain incident management plans, yet CNII-specific incident response protocols remain undefined, creating operational uncertainty and compliance gaps across critical infrastructure sectors. A 2024 cyberattack on the National Bureau of Statistics (NBS) disrupted services for days, including servers of the National Identity Management Commission (NIMC). The lack of consequences or mandated data protection audits shows the weakness of current CNII oversight mechanisms;

Limited Regulatory Inclusion of CSOs in Cyber Oversight:

The Cybercrime Advisory Council (CAC), established under Articles 42 and 43 of the Cybercrimes Act to facilitate multi-stakeholder coordination and strategic oversight, has remained inactive and dominated by security and law enforcement agencies. This limited composition restricts inclusive policy development and undermines public trust in cybersecurity governance. The council was envisioned as a forum to shape policy guidelines, promote information sharing, and advise on preventive measures; it has yet to fulfil this mandate. Notably, the lack of CSO, technical, academic, and digital rights expertise in its composition stands in contrast to global best practices. This mirrors early criticisms of the NDPC, which only saw improved stakeholder alignment after increased CSO participation. Given Nigeria's evolving digital threat landscape, ranging from cybercrime and cyber-espionage to child online abuse, the Council must be revitalized and diversified to meet its statutory objectives, support the implementation of the NCPS, and ensure legitimacy in the CNII governance process.

RECOMMENDATIONS

To strengthen Nigeria's cybersecurity outlook and reinforce public trust in the enforcement of the Designation and Protection of CNII Order, it is important to consider the following:

- **Clarify Legal Definitions and Scope of CNII Offences:** Predictable enforcement begins with legal clarity. Ambiguities in terms like tampering, unauthorized access, and interference create risks of misinterpretation and undermine trust in CNII regulations. Additionally, the absence of statutory safeguards for public interest actors discourages responsible reporting of vulnerabilities. We recommend:
  - Precisely defining key terms to target specific, intentional acts that cause demonstrable harm to national security or the integrity of critical systems;
  - Aligning CNII-related enforcement with the Whistleblower Protection and creating exemptions for ethical hackers, investigative journalists, and technologists operating in the public interest;
  - Embedding proportionality principles in enforcement to ensure that sanctions correspond appropriately to the nature and intent of the infraction.

- **Establish a Public CNII Registry with Transparent Designation Criteria:** Transparent designation is vital for compliance, oversight, and inter-sectoral cooperation. Presently, unclear classification mechanisms create uncertainty among digital service providers and public interest institutions. We recommend:
  - Publishing and maintaining an accessible registry of designated CNII assets;
  - Clear justification for each designation to support public scrutiny;
  - Review and redress procedures should be established to enable institutions or individuals to challenge classifications that they believe are either overly broad or incorrectly applied.

- **Issue Joint Guidelines:** Effectiveness of CNII protection depends on interagency coordination. Currently, gaps in legal alignment across cybersecurity, data protection, and criminal law create enforcement inconsistencies and delay responses to cyber threats. We recommend:
  - Developing and publishing joint implementation guidelines between the ONSA, NDPC, NITDA, and the Attorney General of the Federation (AGF);
  - Ensuring that CNII governance is consistent with the NDPA and the NCPS;
  - Providing courts and enforcement agencies with interpretative guidance that upholds constitutional rights while ensuring system security.

- **Enhance Multi-Stakeholder Inclusion in the CAC:** The council, as mandated by the Cybercrimes Act, helps shape CNII governance but lacks structured input from independent experts and CSOs. We recommend:
  - Expanding the council to include observer roles for digital rights experts, cybersecurity scholars, technologists, and the private sector;
  - Publishing non-sensitive summaries of council discussions and decisions;
  - Engaging the council to inform guidelines, threat assessments, and coordination with civil institutions;

- I**nstitutionalize CNII Roundtables:** CNII protection is an evolving task that requires continuous dialogue among stakeholders to anticipate threats, address compliance gaps, and review enforcement outcomes. We recommend:
  - Conducting an annual CNII Resilience Roundtable convened by ONSA;
  - Include the public and private sectors, digital rights groups, cybersecurity experts, and academia;
  - We are utilizing the roundtables to inform updates to CNII policy, risk mapping efforts, and collaborative responses to threats.

CONCLUSION

As Nigeria deepens its digital economy and asserts continental leadership in cybersecurity, the Designation and Protection of CNII Order, 2024, offers a timely opportunity. A rights-respecting CNII regime is critical, not just for national security, but for public trust, private sector confidence, and democratic legitimacy.

Clear enforcement terms, transparent and proportionate sanctions, and inclusive oversight can reduce abuse and systemic risks while building support for CNII protections. Strengthening coordination across legal, security, and regulatory bodies and institutionalizing input from CSOs and technical experts will ensure governance that is both effective and accountable.

These public interest recommendations by the Data and Digital Rights Coalition, facilitated by AL Nigeria, are intended to contribute to ONSA and other stakeholders' efforts in shaping a CNII framework that secures critical systems without compromising the freedoms, privacy, and trust of the people it is designed to serve.

accountabilitylab
NIGERIA