PROPOSED ACT — A DRAFT WITHOUT LEGAL FORCE

# Critical National Infrastructure & Cyber Resilience Act

| | |
|---|---|
| **Published** | 29 March 2026 |
| **Constitutional basis** | Constitution Article 196 |
| **Ledger hash** | 66189023ebca87201948ea20914801e991204890ecb8201948ea20914801fa88 |

*An Act providing for the mandatory cyber hardening, post-quantum cryptographic standards, and optical air-gapping of sovereign ledgers and public utility grids.*

### Section 1 — Validator Consensus Security

All state consensus validator nodes must be hosted on sovereign hardware with FIPS 140-3 Level 4 HSM key storage and multi-carrier BGP protection.

### Section 2 — SCADA Optical Isolation

Industrial control systems governing offshore wind arrays, port handling gantries, and water desalination must be physically isolated from the public internet via unidirectional optical data diodes.

### Section 3 — Mandatory Incident Reporting

Critical infrastructure operators must report all cyber intrusion attempts to the CSIRT-ALE national desk within sixty minutes of detection.

**Proposed signatory: Director of the National Cybersecurity Directorate**
Draft ACT-2026-09: no legal force


*Founding-phase record without legal force. Aletheia is not a recognised state. The English text is authoritative.*