

Republic of the Philippines  
**HOUSE OF REPRESENTATIVES**  
Quezon City, Metro Manila  
  
**TWENTIETH CONGRESS**  
First Regular Session  
**House Bill No. 4191**



---

**Introduced by Representative**

**BRIAN DANIEL POE LLAMANZARES, PhD, MNSA**

---

**AN ACT STRENGTHENING CYBERSECURITY STANDARDS FOR CRITICAL GOVERNMENT AND PRIVATE INFRASTRUCTURE AND FOR OTHER PURPOSES**

**EXPLANATORY NOTE**

The Philippines' reliance on digital technologies has grown rapidly, shaping government operations, national infrastructure, and vital services. However, this progress has made the country increasingly vulnerable to cyberattacks that threaten national security, public safety, economic stability, and the privacy of citizens.

In recent years, both public and private entities in the country have experienced incidents of ransomware, data breaches, and disruptions to essential services. Such threats are no longer isolated crimes but are now strategic risks that can undermine confidence in government and destabilize critical sectors such as banking, telecommunications, energy, healthcare, and transportation.

Despite existing cybersecurity frameworks, there remains no unified law mandating minimum cybersecurity standards across all critical sectors. As cyber threats evolve, piecemeal or voluntary compliance is insufficient to safeguard essential national systems.

This proposed measure, the **"Critical Infrastructure Cybersecurity Standards Act,"** seeks to establish baseline cybersecurity controls, ensure the creation of Cyber Incident Response Teams (CIRTs) in government agencies, and define sector-specific benchmarks for

resilience. It further strengthens national coordination by mandating the Department of Information and Communications Technology (DICT) to establish a National Cybersecurity Incident Response Framework (NCIRF) and institutionalize mechanisms for threat information-sharing.

The bill also introduces clear enforcement provisions and penalties for non-compliance while supporting capacity-building through training programs, technical assistance funds, and public-private partnerships.

By adopting this measure, the State ensures the protection of essential infrastructure, the integrity of public services, and the trust of the Filipino people in the nation's digital resilience.

In view of the foregoing, the immediate passage of this bill is earnestly sought.

  
HON. BRIAN DANIEL POE LLAMANZARES, PhD, MNSA  
Representative  
FPJ Panday Bayanihan Party-List

Republic of the Philippines  
**HOUSE OF REPRESENTATIVES**

Quezon City, Metro Manila

**TWENTIETH CONGRESS**

First Regular Session

House Bill No. 4191

---

**Introduced by Representative**

**BRIAN DANIEL POE LLAMANZARES, PhD, MNSA**

---

**AN ACT STRENGTHENING CYBERSECURITY STANDARDS FOR CRITICAL  
GOVERNMENT AND PRIVATE INFRASTRUCTURE AND FOR OTHER PURPOSES**

*Be it enacted by the Senate and House of Representatives of the Philippines in Congress  
assembled:*

**SECTION 1. Short Title.** — This Act shall be known as the “Critical Infrastructure Cybersecurity Standards Act.”

**SEC. 2. Declaration of Policy.** — It is the policy of the State to ensure the security, integrity, and resilience of government digital systems and critical national infrastructure against evolving cyber threats. Recognizing the increasing risk posed by cyberattacks to public safety, economic stability, and national security, this Act mandates minimum cybersecurity standards and response mechanisms across sectors.

**SEC. 3. Coverage.** — This Act shall apply to:

- (a) All national government agencies (NGAs), local government units (LGUs), government-owned and controlled corporations (GOCCs), and constitutional commissions; and
- (b) All private entities operating in critical infrastructure sectors, including but not limited to:
  - 1. Banking and financial services;
  - 2. Telecommunications and ICT;
  - 3. Energy and power distribution;

4. Water services;
5. Transportation and logistics;
6. Healthcare and pharmaceutical services;
7. Food and agricultural supply chains.

**SEC. 4. Mandatory Cybersecurity Controls for Government Agencies.** — All government entities must implement the following minimum cybersecurity requirements:

- (1) Zero-Trust Architecture for system access and segmentation;
- (2) Multi-Factor Authentication (MFA) for all administrative and user-level accounts accessing critical systems;
- (3) End-to-End Data Encryption, including at-rest and in-transit encryption for all sensitive and personal data; and
- (4) Regular penetration testing and system vulnerability assessments, conducted semi-annually.

**SEC. 5. Establishment of Cyber Incident Response Teams (CIRTs).** — All government departments and agencies must:

- (a) Create internal Cyber Incident Response Teams (CIRTs) staffed with trained personnel;
- (b) Develop Incident Response Plans in compliance with standards to be issued by the DICT; and
- (c) Coordinate immediately with the National Computer Emergency Response Team (NCERT) and Cybercrime Investigation and Coordinating Center (CICC) in the event of a significant cybersecurity incident.

**SEC. 6. Sector-Specific Cyber Resilience Benchmarks.** — The following sectors shall comply with sectoral minimum benchmarks to be defined by the DICT, in consultation with relevant regulatory agencies:

- (a) **Banking and Finance Sector**, under the regulation of the Bangko Sentral ng Pilipinas (BSP), shall adopt international standards such as ISO 27001 or equivalent, establish real-time fraud detection systems, and operate twenty-four (24) hour Security Operations Centers (SOCs).
- (b) **Telecommunications Sector**, under the regulation of the National Telecommunications Commission (NTC), shall implement endpoint detection, distributed denial-of-service (DDOS) mitigation strategies, and conduct supply chain security audits.
- (c) **Energy Sector**, under the regulation of the Energy Regulatory Commission (ERC), shall adopt network segmentation and supervisory control and data acquisition (SCADA) security protocols.
- (d) **Healthcare Sector**, under the regulation of the Department of Health (DOH), shall maintain secure electronic medical record (EMR) platforms, with encryption and anonymization of patient data.

Benchmarks shall be reviewed and updated every two (2) years to respond to emerging threats.

**SEC. 7. National Cybersecurity Incident Response Framework.** — The DICT shall establish a National Cybersecurity Incident Response Framework (NCIRF) to:

- (a) Define escalation procedures and coordination protocols among the DICT, CICC, PNP-ACG, AFP, and private infrastructure operators;
- (b) Classify cyber incidents by severity level; and
- (c) Enable real-time threat information sharing across government and industry.

**SEC. 8. Enforcement and Compliance Monitoring.** — The DICT, in coordination with regulatory agencies, shall:

- (a) Conduct annual cybersecurity compliance audits for covered entities; and
- (b) Maintain a National Registry of Critical Infrastructure Operators and their compliance status.

**SEC. 9. Penalties for Non-Compliance.** — Entities that fail to comply with the provisions of this Act shall be subject to the following:

- (1) For the first offense, a written warning and the provision of technical assistance;
- (2) For the second offense, a fine of Five Million Pesos (₱5,000,000.00) and temporary suspension of government-issued licenses or accreditations; and
- (3) For the third offense, a fine of Twenty Million Pesos (₱20,000,000.00) and administrative sanctions against responsible officers, including dismissal or disqualification from holding public office.

Public officials may also face disciplinary action under the Civil Service Law for gross neglect of duty.

**SEC. 10. Capacity Building and Technical Support.** — The DICT shall:

- (a) Establish a Cybersecurity Technical Assistance Fund to assist LGUs and small operators;
- (b) Provide certification programs and training modules for public and private sector cybersecurity officers; and
- (c) Develop partnerships with local cybersecurity industries to strengthen the domestic cyber workforce.

**SEC. 11. Appropriations.** — The initial amount of Three Billion Pesos (₱3,000,000,000.00) is hereby appropriated for the following:

- (1) Establishment of the National Cybersecurity Incident Response Framework;
- (2) Creation of CIRTs in government agencies;
- (3) Development of sectoral benchmarks and conduct of compliance audits; and
- (4) Compliance monitoring mechanisms.

Thereafter, appropriations necessary for the implementation of this Act shall be included in the annual General Appropriations Act.

**SEC. 12. Implementing Rules and Regulations (IRR).** — The DICT, in coordination with the Department of National Defense (DND), Department of Finance (DOF), Department of Justice (DOJ), National Telecommunications Commission (NTC), Energy Regulatory Commission (ERC), Bangko Sentral ng Pilipinas (BSP), Department of Health (DOH), and other relevant agencies, shall promulgate the IRR within ninety (90) days from the effectivity of this Act.

**SEC. 13. Separability Clause.** — If any provision of this Act is declared unconstitutional or invalid, the remaining provisions shall remain in full force and effect.

**SEC. 14. Repealing Clause.** — All laws, executive orders, rules, and regulations inconsistent with this Act are hereby amended or repealed accordingly.

**SEC. 15. Effectivity Clause.** — This Act shall take effect fifteen (15) days after publication in the Official Gazette or in at least two (2) national newspapers of general circulation.

*Approved,*

  
HON. BRIAN DANIEL POE LLAMANZARES, PhD, MNSA  
Representative  
FPJ Panday Bayanihan Party-List