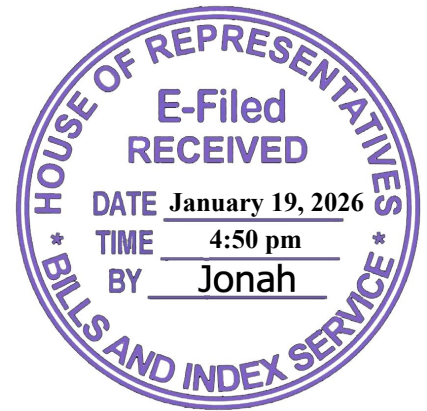


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
1st Regular Session

HOUSE BILL NO. 7203



Introduced by Representative ALEXANDER T. PIMENTEL

EXPLANATORY NOTE

The rapid digital transformation of the Philippines has transitioned our essential services and economic activities into a highly interconnected digital ecosystem. While this shift offers speed and efficiency, it also introduces grave **national security concerns**. Our **Critical Information Infrastructure (CII)** – which includes the digital systems underpinning water, electricity, banking, and telecommunications – is now a primary target for malicious actors, ranging from individual scammers to highly sophisticated **state-backed groups**.

This bill recognizes that the protection of our digital assets is no longer just a technical requirement but a vital component of **national defense**. In line with the **whole-of-government approach** being pursued by our **national defense and intelligence communities**, this measure seeks to ensure the continuous operation of networks vital to the country's security and socio-economic well-being. Any paralysis or disruption of these systems would have a debilitating impact on the safety and stability of the nation.

By establishing a robust national policy framework, we are instituting a **proactive and institutionally cohesive response** to cyberthreats. This bill mandates the adoption of international security standards and a centralized incident reporting mechanism to ensure that our defense and intelligence sectors can effectively monitor and mitigate risks to our digital sovereignty.

For the security and well-being of all Filipinos, the passage of this bill is earnestly sought.


REP. ALEXANDER T. PIMENTEL

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
1st Regular Session

HOUSE BILL NO. 7203

Introduced by Representative ALEXANDER T. PIMENTEL

AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO
ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS
AND INFRASTRUCTURE

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

Section 1. Title. – This Act shall be known as the "**Critical Information Infrastructure Protection Act.**"

Section 2. Declaration of Policy. – It is the policy of the State to protect **Critical Information Infrastructure (CII)** from cyberattacks, data manipulation, and the activities of malicious actors. The State recognizes that securing digital assets is a common objective requiring the **combined efforts of the public and private sectors**, as well as local and international cooperation, to minimize risks to **national security**. The adoption of minimum information security standards is essential for improved risk management and the consistent delivery of vital services.

Section 3. Definition. – For the purpose of this Act, the following definitions shall apply:

a) Critical infrastructure: Assets and networks so vital that their disruption would have a debilitating impact on **national security**, health, or economic well-being.

b) Critical Information Infrastructure (CII): Computer systems and ICT networks necessary for the continuous operation of critical infrastructure services.

c) CII institution: A government agency or private company that owns or operates nationwide or metropolitan-scope CII.

d) Computer Emergency Response Team (CERT): An organization providing incident response services and publishing alerts concerning vulnerabilities.

Section 4. Coverage of Critical Information Infrastructure. – This Act covers public and private CII in industries including: **Banking and finance, Broadcast media, Emergency services, Energy, Health, Telecommunications,**

Transportation, and Water. The Department of Information and Communications Technology (DICT) shall update this list every three years.

Section 5. Adoption of Minimum Information Security Standards. – All covered CII institutions must adopt adequate measures to protect their systems, including compliance with: i) **ISO/IEC 27001** (Information Security Management System); and ii) **ISO 22301** (Business Continuity Management Systems); and iii) Submitting formal certification or an annual **security self-assessment** to the DICT.

Section 6. National Computer Emergency Response Team (NCERT) as the Centralized Mechanism. – All covered CII institutions shall:

- a. Report all information security incidents to the **NCERT**.
- b. Submit an initial incident report within **twenty-four (24) hours of detection**.
- c. Submit post-incident reports regarding the magnitude of the compromise and the response taken.
- d. Participate in **cyber drills** and capacity-building activities.

Section 7. Designation of Personnel with Information Security Credentials. – All government agencies must have at least one personnel with sufficient information security training, preferably at a Division Chief level, to act as the point person for compliance and reporting.

Section 8. Compliance. –

- a. **Government compliance:** Submitting proof of security standards compliance is a prerequisite for **budgetary approval** by the Department of Budget and Management (DBM).
- b. **Private company compliance:** Compliance is a prerequisite for the granting of **regulatory approvals, permits, and licenses**.

Section 9. Implementing Agency. – The **DICT**, through its Cybersecurity Bureau, shall be the implementing agency, responsible for maintaining a database of certifications, prescribing reporting templates, and serving as the custodian of incident reports.

Section 10. Responsibilities of Department Heads. – Heads of departments and sector regulators shall issue the necessary policies to ensure CII institutions under their jurisdiction comply with prevailing security standards.

Section 11. Appropriations. – Funding shall be charged against existing appropriations of covered institutions and other sources identified by the DBM.

Section 12. Penalty. – Non-compliance may result in **administrative, civil, or criminal liability** under the **Cybercrime Prevention Act of 2012** and the **Data Privacy Act of 2012**.

Section 13. Annual Report. – The DICT shall report the status of implementation to the **Office of the President** by April 30 of every year.

Section 14. Separability Clause. – If any provision is declared unconstitutional, the remaining provisions remain in effect.

Section 15. Repealing Clause. – All inconsistent laws or regulations are hereby repealed or modified.

Section 16. Effectivity. – This Act shall take effect fifteen (15) days after publication in the Official Gazette or a newspaper of general circulation.

Approved,