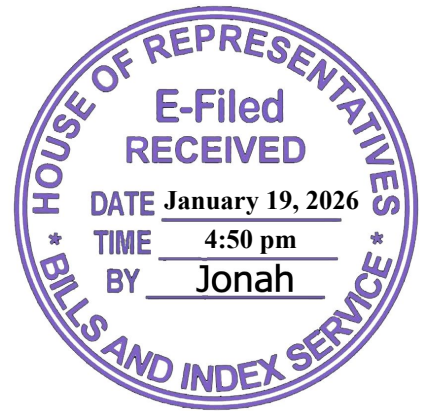


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
1st Regular Session

HOUSE BILL NO. 7202



Introduced by Representative ALEXANDER T. PIMENTEL

EXPLANATORY NOTE

In today's Age of Information, the Philippines is increasingly exposed to sophisticated and rapidly evolving cyber threats. These range from state-sponsored incursions to large-scale data breaches that exploit weaknesses in our defensive posture and erode public trust in digital services and institutions.

During a previous inquiry by the 19th Congress Tri-Committees (TriComm), a disconcerting realization was made regarding how powerless our national agencies are in taking a proactive role in countering cybersecurity threats. Furthermore, there have been various observations of real and imminent threats that have already penetrated the Philippines, highlighting the urgent need for a unified and robust national cybersecurity framework.

This bill responds to these urgent challenges by strengthening our capacity to prevent, detect, and respond to cyber threats through coordinated policy and institutional oversight. The core reforms include:

- **Institutionalizing the Philippine Cybersecurity Council** under the Office of the President to harmonize policy and oversee implementation;
- **Mandating a National Cybersecurity Plan** to strengthen institutional capacity and promote resilience;
- **Establishing a publicly accessible national threat database**, compulsory breach reporting, and enhanced public-private partnerships; and
- **Requiring Internet service providers (ISPs) to enforce hardened device security** and implement rapid malware notification and cleanup schemes.

By codifying clear governance, reporting, and accountability mechanisms, this measure will safeguard critical infrastructure, protect individual privacy, and fortify national resilience in the digital age.

In view of the foregoing considerations, the approval 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. 7202

Introduced by Representative ALEXANDER T. PIMENTEL

AN ACT INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL
CYBERSECURITY FRAMEWORK, AND ESTABLISHING THE PHILIPPINE
CYBERSECURITY COUNCIL AND APPROPRIATING FUNDS THEREFOR

*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 "**Cybersecurity Act.**"

SEC. 2. Declaration of Policy. – The State recognizes the vital role of communication and information in nation building and its inherent obligation to ensure that personal data and communications systems in the government and private sector are secured. The State shall provide Filipinos a **secure, reliable, and trusted cyberspace** through the formulation and enforcement of effective cybersecurity policies and a governance framework that coordinates a proactive, timely, and appropriate response against threats.

SEC. 3. Definition of Terms. – For purposes of this Act:

(a) **Botnet** refers to a network of computers infected by malware under the control of a single attacking party.

(b) **Critical infrastructure** refers to assets, systems, and networks so vital that their destruction would have a debilitating impact on national security, health, or economic well-being.

(c) **Critical Information Infrastructure (CII)** refers to computer systems, ICT networks, and digital assets necessary for the continuous operation of critical infrastructure services.

(d) **Cybersecurity** refers to the collection of resources, processes, and structures to preserve Confidentiality, Integrity, Availability, Non-Repudiation, Authenticity, Privacy and Safety (CIANA-PS) in cyberspace.

SEC. 4. Philippine Cybersecurity Council. – The Philippine Cybersecurity Council is hereby established as an **inter-agency body administratively attached to the Office of the President**. The Council shall be headed by the Director-General of the National Intelligence Coordinating Agency (NICA) and co-chaired by the Executive Secretary and the Secretary of the Department of Information and Communications Technology (DICT). Members shall include the Secretaries of

various departments, including the **Governor of the Bangko Sentral ng Pilipinas (BSP)**.

SEC. 5. Powers and Functions. – The Council shall be the **primary authority** on cybersecurity matters, including assessing vulnerabilities, capacity building, issuing security protocols, and enhancing public-private partnerships for information sharing.

SEC. 6. Meetings of the Council. – The Council shall hold regular meetings every quarter and special meetings as necessary.

SEC. 7. Reportorial Requirement. – The Council shall submit a **quarterly report** to the President and to Congress on the state of cybersecurity threats.

SEC. 8. Cybersecurity Bureau. – The DICT shall strengthen its Cybersecurity Bureau (CSB), expanding the operations of the National Computer Emergency Response Team (NCERT) and the National Security Operations Center (NSOC) on a **24-hour basis**.

SEC. 9. Modernization Program. – The Council shall develop a modernization program to strengthen monitoring and provide a **centralized incident response system** for government agencies and local government units (LGUs).

SEC. 10. Reporting of Data Breach. – Government and private entities are **required to report all kinds of data breaches** occurring in their jurisdiction to the Council within a reasonable period of time.

SEC. 11. Mandatory Notification by Internet Service Providers. – All ISPs are required to implement a **malware notification scheme** and perform immediate cleanup of detected malwares. ISPs must also harden Customer Premise Equipment (CPE) by changing default passwords and disabling unused ports.

SEC. 12. Threats and Baseline Assessments. – The Council shall develop the capability to automatically scan government and CII assets for vulnerabilities and provide risk scores to owners for mitigation.

SEC. 13. National Cybersecurity Threat Database. – The Council shall develop a **publicly accessible database** of threats, curated based on a common vulnerability scoring system (CVSS).

SEC. 14. Standards to Protect Inter-Domain Internet Protocol (IP) Routing Protocol. – The Council shall adopt and implement standards, particularly **Border Gateway Protocol (BGP)**, to secure inter-domain routing.

SEC. 15. Partnership with Digital Online Platforms. – The Council shall initiate partnerships with social media platforms to create protocols for reporting and mitigating **misinformation and online harms**.

SEC. 16. Multi-Disciplinary Approach. – All government agencies and LGUs are enjoined to develop their own cybersecurity strategies consistent with this Act.

SEC. 17. National Cybersecurity Awareness Month. – The month of **October** is hereby declared as "National Cybersecurity Awareness Month".

SEC. 18. The National Cybersecurity Plan. – A National Cybersecurity Plan (NCSP) shall be formulated by the Council to strengthen institutional capacity and promote resilience.

SEC. 19. Critical Information Infrastructure (CII). – This Act covers CIIs in sectors including **Banking and Finance, Broadcast Media, Emergency Services, Energy, Health, Telecommunications, Transportation, and Water.**

SEC. 20. Adoption of Minimum Information Security Standards. – Covered CII institutions must adopt and implement adequate measures, such as **ISO/IEC 27001 (ISMS)** and **ISO 22301 (BCMS).**

SEC. 21. Prosecution of Cyber Offenders. – The DOJ, in coordination with the NBI and PNP, shall establish specialized units for the investigation and prosecution of cybercrime.

SEC. 22. Penal Provisions. – Any violation of Sections 10 and 11, **after due notice and hearing**, shall be penalized with **imprisonment of six (6) months to two (2) years** or a fine of up to **One Million Pesos (P1,000,000.00)**, or both.

SEC. 23. Appropriations. – The necessary funds shall be included in the annual General Appropriations Act.

SEC. 24. Implementing Rules and Regulations. – The NICA and DICT shall jointly formulate the IRR within ninety (90) days from approval.

SEC. 25. Separability Clause. – If any provision is held invalid, others remain in effect.

SEC. 26. Repealing Clause. – All inconsistent laws or regulations are hereby repealed or modified.

SEC. 27. Effectivity. – This Act shall take effect fifteen (15) days after publication in the Official Gazette or in two (2) newspapers of general circulation.

Approved,