

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. **5592**



Introduced by: **REP. SALVADOR A. PLEYTO, SR.**

EXPLANATORY NOTE

The Philippines, with its rapidly growing digital economy and expanding reliance on information and communications technology (ICT) for governance, commerce, and essential services, faces significant cybersecurity vulnerabilities.

Current national efforts, while present, often suffer from fragmented governance, inconsistent implementation across sectors, and a lack of a unified, statutory framework with dedicated funding.

The primary objective of this Bill is to create a robust, resilient, and unified national cybersecurity posture to protect the nation's interests, critical services, and the data privacy of its citizens.

The Bill establishes the Philippine Cybersecurity Council (PCC), chaired by the Secretary of the DICT and composed of key cabinet members and regulators (DND, NSA, BSP, etc.). This Council is mandated to be the single, highest policymaking and coordinating body, ensuring strategic alignment and rapid decision-making across government agencies and the private sector.

The disruption of essential services—such as banking, power, telecommunications, and healthcare—due to a cyberattack poses a severe threat to national security and public safety. The Bill mandates minimum security standards, regular risk assessments, and compulsory incident reporting for all identified Critical Information Infrastructure (CII) entities. This ensures that the most vital sectors are held to a non-negotiable standard of security, enhancing the national resilience against systemic attacks.

A reactive approach to cyber threats is unsustainable. The formulation and regular updating of a comprehensive National Cybersecurity Plan (NCSP) is included to institutionalize core programs for incident management, capacity building, and information sharing.

Effective national cybersecurity requires sustained investment in technology, training, and skilled personnel. This Bill ensures that the implementation of the Act, the operations of the PCC, and the necessary cybersecurity programs are adequately funded through appropriations included in the annual General Appropriations Act. This provides the necessary financial stability and legal backing essential for long-term strategic success.

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



SALVADOR A. PLEYTO, SR.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. **5592**

Introduced by: **REP. SALVADOR A. PLEYTO, SR.**

AN ACT
INSTITUTIONALIZING POLICIES FOR A SECURE, TRUSTED, AND
RELIABLE CYBERSPACE, STRENGTHENING THE GOVERNANCE OF
CYBERSECURITY, ESTABLISHING FOR THE PURPOSE 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 "Philippine Cybersecurity Act of 2025."

SEC. 2. *Declaration of Policy.* It is hereby declared the policy of the State to:

1. Ensure a secure, trusted, and reliable cyberspace as a key pillar for national security, economic prosperity, and social well-being.
2. Protect Critical Information Infrastructures (CII) from cyber threats and attacks.
3. Foster a culture of cybersecurity awareness and responsibility among the government, private sector, and the general public.
4. Strengthen the governance, coordination, and cooperation among all sectors in cybersecurity matters.
5. Promote the development of local cybersecurity talent and technology.

SEC. 3. *Definition of Terms.* - As used in this Act:

1. Cybersecurity refers to the collection of tools, policies, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

2. Critical Information Infrastructure (CII) refers to systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.
3. Cyber Threat refers to any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via cyberspace.
4. National Cybersecurity Plan (NCSP) refers to the strategic framework and roadmap for the country's cybersecurity program.

SEC. 4. *Establishment of the Philippine Cybersecurity Council.* - There is hereby created a Philippine Cybersecurity Council (PCC), hereinafter referred to as the "Council," which shall be the principal body responsible for policy direction, strategic planning, and overall coordination of the national cybersecurity efforts.

SEC. 5. *Composition of the Council.* - The Council shall be composed of the following:

Chairperson	Secretary of the Department of Information and Communications Technology (DICT)
Vice-Chairperson	Secretary of National Defense (SND)
Members	National Security Adviser (NSA) Secretary of the Department of the Interior and Local Government (DILG) Secretary of the Department of Foreign Affairs (DFA) Governor of the Bangko Sentral ng Pilipinas (BSP) Commissioner of the National Privacy Commission (NPC) A representative from the private sector, appointed by the President, with proven expertise in cybersecurity.

SEC 6. *Powers and Functions of the Council.* - The PCC shall have the following powers and functions:

1. Formulate and regularly update the National Cybersecurity Plan (NCSP).

2. Ensure the harmonized implementation of cybersecurity policies and programs across all government agencies and sectors.
3. Establish national standards and protocols for cybersecurity risk management, incident response, and protection of CII.
4. Oversee the establishment and operation of a national computer emergency response team (CERT) system.
5. Promote international cooperation in cybersecurity matters, including information sharing and capacity building.
6. Recommend necessary legislative measures to further strengthen the country's cybersecurity posture.

SEC. 7. *Cybersecurity Policy and Programs.* - The Council, through the DICT, shall institutionalize the following policies and programs:

1. Critical Information Infrastructure (CII) Protection: Mandating regular risk assessments, compliance with minimum security standards, and mandatory reporting of significant cyber incidents for all CII entities, which shall be identified by the DICT in consultation with relevant sector regulators.
2. Cybersecurity Awareness and Education: Implementing a national program to raise public awareness and developing cybersecurity curricula for educational institutions.
3. Cyber Incident Management: Establishing a coordinated national framework for detection, analysis, containment, recovery, and information sharing for cyber incidents.
4. Government Network Security: Implementing mandatory baseline security controls, penetration testing, and continuous monitoring across all government information systems and networks.

SEC. 8. *Data and Information Sharing.* - Government agencies and CII entities shall, under rules to be promulgated by the Council, share timely and relevant cyber threat and incident information to enhance collective defense, while upholding the principles of privacy and confidentiality under the Data Privacy Act of 2012.

SEC. 9. *Appropriations.* - The amount necessary to carry out the initial implementation of this Act shall be charged against the current year's appropriations of the DICT and other relevant agencies. Thereafter, such sums as may be necessary for the continued implementation of this Act shall be included in the annual General Appropriations Act.

SEC. 10. *Implementing Rules and Regulations.* - Within ninety (90) days from the effectivity of this Act, the DICT, in consultation with the members of

the Council and relevant stakeholders, shall promulgate the necessary rules and regulations for the effective implementation of this Act.

SEC. 11. *Separability Clause.* - If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

SEC. 12. *Repealing Clause.* - All laws, decrees, orders, rules, and regulations, or parts thereof, inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 13. *Effectivity.* - This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,