

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 6818



Introduced by **ANG PROBINSYANO**
Party-List Representative Alfred Delos Santos

EXPLANATORY NOTE

Cyberspace, unlike conventional physical space, is particularly difficult to secure. Malicious and sophisticated perpetrators can launch a wide range of threats and hazards, both physical and cyber, from anywhere in the world. Certain groups, ranging from criminal networks to hostile organizations, take advantage of weaknesses in information and communications technology (ICT) systems to steal data and resources. They are also developing increasingly sophisticated methods to disrupt, sabotage, and even terrorize societies by targeting the delivery of essential services. The increasing dependence on cyber networks to provide essential services has compounded vulnerabilities and weaknesses. This interconnectedness between cyberspace and critical infrastructure exposes the country to risks of wide-scale attacks that could disrupt services, paralyze the economy, and endanger the lives of millions of Filipinos, particularly those in marginalized sectors who rely most heavily on government services.

The Philippines has consistently ranked among the top countries in Southeast Asia for cyber threats, with government websites, financial institutions, and private businesses reporting surges in phishing, ransomware, and defacement attacks in recent years¹. In recent years, banks and online platforms have reported significant increases in identity theft and ransomware cases, undermining public trust in digital transactions and exposing sensitive personal data to exploitation. Globally, critical infrastructure such as healthcare

¹ Kaspersky Report published in *BusinessMirror* (May 28, 2024)
<https://businessmirror.com.ph/2024/05/28/phl-faces-highest-rise-in-cyber-threats-in-region/> |
Manila Standard (February 18, 2025)– *PH cyber threat ranking rises 10 spots to 66th*
<https://manilastandard.net/business/314559217/ph-cyber-threat-ranking-rises-10-spots-to-66th.html>

systems, transportation networks, and power grids have been subject to cyberattacks, demonstrating that no sector is immune to these risks².

At present, the country's legal framework is anchored on Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012. This law defines cybercrimes such as hacking, identity theft, cybersex, and child pornography, among others and provides mechanisms for investigation, and penalties. However, it is primarily focused on the criminalization of offenses related to cybersecurity rather than the protection of critical infrastructure. Complementing this law is the National Cybersecurity Plan 2023–2028 of the Department of Information and Communications Technology (DICT), which serves as a strategic policy framework but is not a law. The plan aims to strengthen national cyber defense, protect government networks, and secure critical information infrastructure, identifying priority sectors such as government, banking, transportation, energy, and healthcare.

Despite these measures, there remains a significant legislative gap. The Philippines has yet to enact a comprehensive law on critical infrastructure protection.

In light of these increasing risks and their potential impact, there is a clear demand for a more capable, cohesive, and institutionalized cybersecurity defense system. Strengthening the security and resilience of our cyberspace is a national imperative that must be promptly addressed. This bill seeks to establish a **National Cybersecurity and Infrastructure Protection Agency**, tasked with implementing cybersecurity measures and safeguarding critical infrastructure. The agency will serve as the central body to coordinate efforts across government, industry, and civil society, ensuring that frontline services are protected, sensitive information is secured, and public trust in digital transactions is reinforced. By creating a single institution to address this national concern, the Philippines will be better equipped to advance its cybersecurity agenda, protect its people, and secure its future in the digital age.

It is for these foregoing premises that approval of this bill is earnestly sought.


ALFRED C. DELOS SANTOS
Representative, Ang Probinsyano Partylist

² World Economic Forum (October 13, 2025) - <https://www.weforum.org/stories/2025/10/dangerous-blindspot-in-infrastructure-cybersecurity/>

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 6818

Introduced by **ANG PROBINSYANO**
Party-List Representative Alfred Delos Santos

AN ACT
STRENGTHENING CYBERSECURITY AND CRITICAL INFRASTRUCTURE
PROTECTION, CREATING THE CYBERSECURITY AND INFRASTRUCTURE
PROTECTION COMMISSION, AND FOR OTHER PURPOSES

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

SECTION 1. *Short Title.* – This Act shall be known as the “Cybersecurity and Infrastructure Protection Act of 2025.”

SECTION 2. *Declaration of Policy.* – Article II, Section 4 of the 1987 Constitution declares that “*the prime duty of the Government is to serve and protect the people.*” Towards this end, the State shall adopt measures that safeguard the rights and interests of the people by ensuring the security of both physical and digital environments. The State shall guarantee that essential services are not impeded and that the welfare and well-being of all citizens are protected in cyberspace.

Equally, Article XIV, Section 10 of the Constitution provides that “*science and technology are essential for national development and progress. The State shall give priority to research and development, invention, innovation, and their utilization; and to science and technology education, training, and services. It shall support indigenous, appropriate, and self-reliant scientific and technological capabilities, and their application to the country’s productive systems and national life.*”

In recognition of the role of science and technology in ensuring national security, the State shall invest in programs that address emerging cyber threats,

strengthen resilience against attacks, and build indigenous capabilities for self-reliance in cybersecurity and infrastructure protection.

SECTION 3. Objectives. – The objectives of this Act are as follows:

- a) Establish a dedicated agency tasked with improving cybersecurity and protecting critical infrastructure against threats in cyberspace.
- b) Enhance Information and Communication Technology (ICT) frameworks to ensure the uninterrupted delivery of essential services.
- c) Safeguard the information of the State and its citizens, and build national capacity to defend against cyber threats, sabotage, and acts of terrorism.
- d) Invest in and capacitate Filipino personnel to develop a self-reliant and globally recognized cybersecurity workforce.
- e) Consolidate and institutionalize existing efforts to protect the State's cyber interests, including the effective implementation of the National Cybersecurity Plan 2023–2028.

SECTION 4. Definition of Terms. – For the purposes of this Act, the following definitions shall apply:

- a. *Computer* refers to any electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, including data storage facilities or communications facilities directly related to or operating in conjunction with such device.
- b. *Computer system* refers to an arrangement of interconnected computers that are designed to perform one or more specific functions, and including:
 - i. an information technology system; and
 - ii. an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;
- c. *Critical infrastructure* refers to the computer systems, networks, programs, data, or traffic data, whether physical or virtual, that are

vital to the State, such that their incapacity, destruction, or interference would have a debilitating impact on national or economic security, public health, safety, or any combination thereof.

- d. *Cybersecurity* refers to the state in which a computer or computer system is protected from unauthorized access or attack.
- e. *Cybersecurity incident* refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardizes or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.
- f. *Cybersecurity program* refers to any computer program designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of a computer or computer system.
- g. *Cybersecurity threat* refers to any act or activity, whether known or suspected, carried out on or through a computer or computer system that may imminently jeopardize or adversely affect, without lawful authority, the cybersecurity of that or another system.

SECTION 5. *Cybersecurity and Infrastructure Protection Commission.* – There is hereby created the *Cybersecurity and Infrastructure Protection Commission*, hereinafter referred to as the *Commission*. The Commission shall be independent and autonomous, with the status of a national government agency attached to the Office of the President. It shall be headed by a Cybersecurity Commissioner, who shall exercise overall supervision and control of the Commission's operations, programs, and personnel.

SECTION 6. *Duties and Responsibilities.* – The Commission shall have the following duties and functions to strengthen cybersecurity and protect critical infrastructure nationwide:

- a. The Commission shall oversee and promote the security of computers, networks, and information systems in the Philippines, ensuring resilience against unauthorized access, disruption, and attacks. It shall advise the Government and other public authorities on national needs, priorities, and policies relating to cybersecurity and infrastructure protection, and shall continuously monitor threats originating within or outside the country.
- b. The Commission shall respond to cybersecurity incidents that threaten national security, defense, the economy, foreign relations, public health, public order, public safety, or the delivery of essential services, regardless of whether such incidents occur domestically or internationally. It shall identify and designate critical infrastructure

and regulate its owners and operators to ensure compliance with cybersecurity standards and protocols.

- c. The Commission shall represent the Government in international forums and negotiations on cybersecurity issues, and shall cooperate with cyber emergency response teams (CERTs) and similar bodies in other countries or territories to address cross-border incidents. It shall establish and enforce national standards for cybersecurity products and services, including recommended levels of protection for hardware and software, and may implement certification or accreditation schemes to ensure compliance.
- d. The Commission shall promote, develop, and maintain professional competencies and standards for individuals working in the field of cybersecurity, while supporting the advancement of technology, research, and innovation in this area. It shall also lead nationwide awareness campaigns to highlight the importance of cybersecurity and encourage responsible digital practices among citizens, businesses, and government institutions.
- e. Finally, the Commission shall aid in the effective implementation of existing cyber-related laws, including but not limited to Republic Act No. 10175, otherwise known as the *Cybercrime Prevention Act of 2012*; Republic Act No. 8792, otherwise known as the *E-Commerce Act of 2000*; and Republic Act No. 10173, otherwise known as the *Data Privacy Act of 2012*.

SECTION 7. Powers and Functions of the Commission. – To effectively carry out its mandate, the Cybersecurity and Infrastructure Protection Commission shall exercise the following powers and functions:

- a. The Commission shall have the authority to issue rules, regulations, and directives necessary to implement the provisions of this Act, including the adoption of minimum cybersecurity standards for government agencies, critical infrastructure operators, and private entities handling sensitive data. It shall conduct audits, inspections, and assessments of cybersecurity practices across public and private institutions, and may impose administrative sanctions for non-compliance with established standards.
- b. The Commission shall establish and operate a National Cybersecurity Operations Center to serve as the central hub for monitoring, detecting, and responding to cyber threats and incidents. It shall coordinate with law enforcement agencies, the

Armed Forces of the Philippines, and other relevant government bodies to investigate and prosecute cybercrimes, and may recommend the suspension or shutdown of systems that pose imminent risks to national security or public safety.

- c. The Commission shall have the power to designate and classify critical infrastructure sectors, and to require operators of such infrastructure to adopt resilience measures, including incident response protocols, redundancy systems, and disaster recovery plans. It may compel cooperation from government agencies and private entities in the sharing of threat intelligence, vulnerability assessments, and incident reports, subject to data privacy safeguards under Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012.
- d. The Commission shall enter into agreements and partnerships with international organizations, foreign governments, and global cybersecurity institutions to strengthen cross-border cooperation, intelligence sharing, and capacity-building. It shall also administer grants, training programs, and scholarships to develop a pool of highly skilled Filipino cybersecurity professionals, and may accredit institutions offering specialized education and training in cybersecurity and infrastructure protection.

SECTION 8. *Cybersecurity Commissioner.* – There shall be one (1) “Cybersecurity Commissioner”, hereinafter referred to as the “Commissioner”. The Commissioner shall be a natural-born citizen of the Philippines; have occupied positions of responsibility and leadership in information and communications technology (ICT) organizations or institutions; of good moral character; and not have been convicted of any crime involving moral turpitude. The Commissioner shall serve as the head and official representative of the Commission and shall oversee the overall implementation of this Act.

SECTION 9. *National Cybersecurity Plan and Framework.* – There shall be created a National Cybersecurity Plan which aims to address the cybersecurity threats and create measures that will lead to a secure and resilient Philippine cyberspace. It shall be the institutional framework and foundation that shall be implemented by the Commission, together with other partner agencies involved in cybersecurity. Further, the National Cybersecurity Plan and Framework shall include, but not limited to:

- e. Cybersecurity Assessment and Compliance
- f. National Cybersecurity Drills and Exercises

- g. National Database for Monitoring and Reporting
- h. Cybersecurity Enhancement Programs in Government Agencies and Local Government
- i. Threat Intelligence and Analysis Program
- j. Basic Cyber Emergency Response Program
- k. National Common Information and Communications Technology (ICT) Equipment Security Evaluation and Certification Project
- l. Update of Cybersecurity Software Licenses
- m. Installation of Cybersecurity Hubs
- n. Protection of Electronic Government (e-Gov) Services and Transactions

SECTION 10. *National Cyber Emergency Response Protocol.* – There shall be an established National Cyber Emergency Response Protocol, hereinafter referred to as “Protocol”. The Commission, in coordination with the Advisory Council, shall formulate the Protocol to aid government agencies, sectors, and organizations in the event of cybersecurity incidents or cybersecurity threats.

SECTION 11. *Capacity Building and Capability Development.* – The government, through the Commission, shall endeavor to invest in capacity building, capability development programs, competitive staff remuneration, cyber training facilities, and cybersecurity and research development. The Commission shall engage and collaborate with the academe and other institutions to support the development of cybersecurity specialists through collaboration and development.

Further, the Commission, in the interest of developing qualified and competent cybersecurity professionals, shall provide for scholarships for training and development through short executive courses or postgraduate degree programs.

SECTION 12. *Advisory Council.* – There shall be an Advisory Council which shall be composed of the Secretary of the Department of Information and Communications Technology (DICT), as Chairman, and the Secretaries of Department of Justice (DOJ), Department of Science and Technology (DOST), Department of National Defense (DND), Department of Interior and Local Government (DILG), Director-General of the National Security Council, Chief of the Philippine National Police, Director of the National Bureau of Investigation (NBI), and the Chairperson of both Senate and House Committees dealing with security and technology.

The Council shall meet once every three (3) months, or as often as may be necessary, upon the call of its chairman, advise and be consulted by the Commission on important matters relating to cybersecurity, infrastructure protection, and development.

The Council may form task forces which shall convene between the meetings of the Council. The Commission shall provide the technical support required by the Council to function according to this Act.

SECTION 13. *Appropriations.* – An initial fund of P500 million shall be appropriated for the immediate implementation of this Act. Thereafter, such sums as may be necessary for the continued operations and maintenance of the programs shall be included in the annual General Appropriations Act.

SECTION 14. *Separability Clause.* – If any provision or part of this Act is held invalid or unconstitutional, the remaining provisions or parts unaffected shall remain in full force and effect.

SECTION 15. *Repealing Clause.* – All laws, executive orders, presidential decrees or issuances, letters of instruction, administrative orders, rules, and regulations contrary to or inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

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

Approved,