Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

Twentieth Congress
First Regular Session

HOUSE BILL NO. 9

Introduced by Representatives Ferdinand Martin G. Romualdez, Andrew Julian K. Romualdez and Jude A. Acidre

EXPLANATORY NOTE

In an era when digital connectivity underpins our economy, governance, and daily lives, the Philippines faces increasingly sophisticated cyber threats—from state-sponsored incursions to widespread data breaches—that exploit gaps in our defensive posture and erode public trust. This bill responds to those challenges by unifying and strengthening our national cyber architecture.

The core reforms of the proposed bill are the following:

- Institutionalizing the Philippine Cybersecurity Council under the Office of the President to harmonize policy and oversee implementation;
- Mandating a National Cybersecurity Defense Plan with regular reviews to ensure agility against evolving threats;
- Establishing a publicly accessible threat database, compulsory breach reporting, and enhanced public-private partnerships; and
- Requiring Internet service providers to enforce hardened device security and rapid malware notification and cleanup.

By codifying clear governance, reporting, and accountability mechanisms—and by investing in continuous workforce development and international cooperation—this measure will safeguard critical infrastructure,

protect individual privacy, and fortify our nation's resilience in cyberspace. Immediate passage is essential to secure the Philippines' digital future.

Further, we acknowledge Representatives Keith Micah "Atty. Mike" D.L. Tan, Jaime R. Fresnedi, and Charisse Anne C. Hernandez for filing this bill during the 19th Congress.

In view of the foregoing considerations, approval of this bill is earnestly sought.

FERDINAND MARTIN G. ROMUALDEZ

JUDE A. ACIDRE

ANDREW JULIAN K. ROMUALDEZ

Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

Twentieth Congress
First Regular Session

HOUSE BILL NO. 9

Introduced by Representatives Ferdinand Martin G. Romualdez, Andrew Julian K. Romualdez and Jude A. Acidre

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

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 Act."

SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of communication and information in nation building. The State also recognizes its inherent obligation to ensure that personal data information and communications systems in the government and the private sector are secured and protected. Towards this end, the State shall provide Filipinos a secure, reliable, and trusted cyberspace through the formulation and enforcement of effective cybersecurity policies, and establishment of a governance framework that shall efficiently

coordinate government agencies and relevant sectors in the preparation of proactive, timely, and appropriate response against cybersecurity threats.

SEC. 3. *Definition of Terms.* -

(a) *Botnet or "robot network"* refers to a network of computers infected by malware that is under the control of a single attacking party;

(b) *Critical infrastructure* refers to assets, systems, and networks, whether physical or virtual, that are considered so vital that their destruction or disruption would have a debilitating impact on national security, health and safety, or economic well-being of citizens, or any combination thereof.

(c) *Critical Information Infrastructure (CII)* refers to computer systems, ICT information and communications technology (ICT) networks, and digital assets that are necessary for the continuous operation and delivery of the country's critical infrastructure services.

(d) *CII institution* refers to a government agency or a private company that owns, operates, controls, and/or maintains critical information infrastructure, and whose operation is nationwide in scope and/or covers metropolitan centers, including Metro Manila, Metro Cebu, Metro Davao, and, by 2025, Metro Cagayan de Oro, or as defined and updated by the National Economic Development Authority (NEDA) or the Philippine Statistics Authority (PSA).

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

(f) *Cybersecurity governance* refers to the strategic approach that governs the implementation and maintenance of cybersecurity measures, which are intended to protect information and digital assets from cyber threats and unauthorized access;

(g) *Cyberspace* refers to complex environment resulting from the interaction of people or software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form;

(h) *Distributed denial of service (DDoS) attack* refers to a variant of a denial of service (DoS) attack that employs very large numbers of attacking computers to overwhelm the target with bogus traffic;

(i) *Internet of Things (IoT) botnets* refer to a network of compromised or infected Internet of Things devices that can be remotely controlled by cybercriminals for malicious purposes;

(j) *Malware* refers a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants; and

(k) *National Cybersecurity Plan* refers to the security policies, procedures, and controls required to protect the country against threats and risk.

SEC. 4. *Philippine Cybersecurity Council.* – The Philippine Cybersecurity Council is hereby established, which shall be 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). It shall be composed of the following officials as members:

(a) Secretary of the Department of Foreign Affairs (DFA);

(b) Secretary of the Department of Finance (DOF);

(c) Secretary of the Department of Science and Technology (DOST);

(d) Secretary of the Department of Interior and Local Government (DILG);

(e) Secretary of the Department of Justice (DOJ);

(f) Secretary of the Department of Energy (DOE);

(g) Secretary of the Department of National Defense (DND);

(h) Secretary of the Department of Transportation (DOTr);

(i) Secretary of the Presidential Communication Operations Office (PCOO);

(j) Secretary of the Presidential Communications Development and Strategic Planning Office (PCDSPO)

(k) Commissioner of the National Telecommunications Commission (NTC);

(l) Director of the National Bureau of Investigation (NBI);

(m) Chief of the Philippine National Police (PNP);

(n) Chief of Staff of the Armed Forces of the Philippines;

(o) Chairman of the National Privacy Commission (NPC);

(p) Executive Director of the Anti-Terrorism Council-Program Management Center (ATM-PMC);

(q) Executive Director of the Cybercrime Investigation and Coordinating Center (CICC); and

(r) Governor of the Bangko Sentral ng Pilipinas (BSP) as members.

The Office of the Deputy Director General (ODDG) for Cyber and Emerging Threats established under NICA shall serve as Secretariat to the Council.

The Council may invite concerned public and private agencies or entities to participate, complement, and assist in the performance of its functions.

The Council shall collaborate with the Anti-Terrorism Council (ATC) on matters relating to cyber- terrorism.

SEC. 5. *Powers and Functions*. – The Council shall be the primary authority to exercise powers and functions that would address all cybersecurity related matters. It shall perform the following functions:

(a) Assess the vulnerabilities of the country's cybersecurity;

(b) Capacity building for the purpose of responding to cybersecurity threats and emergencies;

(c) Issue updated security protocols to all government employees in the storage, handling and distribution of all forms of documents and communications based on the best practices and update the same as necessary;

(d) Enhance the public-private partnership in the field of information sharing involving cyberattacks, threats and vulnerabilities to cyber threats;

(e) Conduct periodic strategic planning and workshop activities that will reduce the country's vulnerabilities to cyber threats;

(f) Direct its member agencies and appropriate agencies to implement cybersecurity measures as may be required by the situation;

(g) Serve as the country's coordinating arm on domestic, international, and transnational efforts pertaining to cybersecurity;

(h) Make such recommendations and/or such other reports as the president may from time to time require; and

(i) Perform such other functions as may be necessary.

SEC. 6. *Meetings of the Council.* – The Council shall hold regular meeting every quarter and such special meetings as may be necessary upon the request of the chairman or upon the request of at least two (2) of its members.

SEC. 7. *Reportorial Requirement* – The Council shall submit quarterly report, or as often as may be necessary, to the President of the Philippines and to Congress on the state of cybersecurity threats and other related information.

SEC. 8. *Cybersecurity Bureau.* – The DICT shall develop an effective and efficient cybersecurity organization and structure to strengthen its Cybersecurity Bureau (CSB). It shall expand the operations of the National Computer Emergency Response Team (NCERT), which shall be tasked to respond on cybersecurity incidents and conduct investigations; and the National Security

Operations Center (NSOC), which shall be primarily responsible in monitoring critical information assets in cyberspace, perform vulnerability assessment and penetration testing (VAPT) services, and conduct baseline assessment of cybersecurity posture of agencies of government.

The NCERT and the NSOC shall be operated and staffed on a twenty-four (24) hour basis under the CSB.

SEC. 9. *Modernization Program.* – The Council shall, in consultation with the relevant agencies of government, develop a modernization program that will strengthen the monitoring of cybersecurity of national government agencies and local government units (LGUs). The modernization program shall include the provision of a centralized incident response system for government that allows the delegation of incident tickets to government agencies and LGUS to monitor their progress and ensure a single view of all cybersecurity incidents.

SEC. 10. *Reporting of Data Breach.* – Government institutions, agencies, instrumentalities, including government owned and controlled corporations, private corporations, companies and business establishments, operating wholly or partly in the Philippines, are required to report to the Council, within a reasonable period of time, all kinds of data breach occurring in their jurisdiction. The Council shall conduct trainings on cybersecurity to all stakeholders for the effective implementation of this provision.

SEC. 11. *Mandatory Notification by Internet Service Providers for Malware Infection and Internet of Things (IoT) Botnets.* – To mitigate the threat of malware and botnets in the country, all internet service providers (ISPs) shall be required to implement a malware notification scheme, including internet of things (IoT) Botnets, and immediate performance of a cleanup of malwares detected.

ISPs are mandated to conduct effective countermeasures including the following:

(a) Performing cybersecurity hygiene in their Customer Premise Equipment (CPE) such as changing the CPE default password, disabling unused ports, and other hardening measures for CPE;

(b) Notifying those infected by malware and providing clear but concise instructions on how to clean their devices; and

(c) Complying with requests for quarantining network segments which are attempting a distributed denial of service (DDoS) attack or identified as part of a command-and-control structure of a ransomware, malware, or botnet.

SEC. 12. *Threats and Baseline Assessments of Government Cyberspace Assets.* – The Council shall develop capability to automatically scan all government and critical information infrastructure assets exposed in the internet for their vulnerabilities and provide a risk score to these scanned threats. The scores and vulnerabilities scanned shall be kept confidentially and shall be provided to the owners of the scanned cybersecurity assets. Owners of these compromised assets shall report to the Council how vulnerabilities were mitigated.

The Council shall develop and/or acquire the necessary tools to ensure that the assessments are stored and disseminated to all government agencies. Private security research shall be allowed to report their own findings subject to the necessary guidelines that the Council shall issue for responsible disclosure of vulnerabilities. Legal protection shall be provided to any security researcher disclosing any vulnerability found in any cyberspace asset.

SEC. 13. *National Cybersecurity Threat Database.* – The Council shall develop a national cybersecurity threat database, which shall be accessible to the

public. The list of threats shall be curated based on the category of the threat and the type of the threat based on their common vulnerability scoring system (CVSS), category and type. The threat database shall be updated regularly.

The Council shall develop and maintain a website to inform the public of the latest trends in cybersecurity and to issue advisories.

SEC. 14. *Standards to Protect Inter-Domain Internet Protocol (IP) Routing Protocol.* – The Council shall, in consultation with the NTC, DICT, DOST, and telecommunications providers, adopt and implement standards for securing inter-domain internet protocol (IP) routing protocol, particularly Border Gateway Protocol (BGP) to attain national compliance for securing inter-domain routing.

SEC. 15. *Partnership with Digital Online Platforms.* – The Council shall initiate robust and meaningful partnerships with digital online and social media platforms to create a mutually acceptable protocol for reporting, correcting and mitigating misinformation, and online harms in line with the need to regulate digital online platforms, including social media platforms.

SEC. 16. *Multi-Disciplinary Approach.* – All government agencies, including LGUs, are enjoined to improve and develop their own cybersecurity strategies, sub-plans, and teams consistent with the provisions of this Act.

SEC. 17. Declaring the Month of October as Cybersecurity Awareness Month. - The month of October of every year is hereby declared as "National Cybersecurity Awareness Month".

Pursuant to the observance of National Cybersecurity Awareness Month, an annual program of activities shall be prepared and implemented, with the NICA and the DICT as lead agencies. They are authorized to call upon any department, bureau, office, agency, or instrumentality of the government,

including government-owned or controlled corporations, for any assistance as may be needed.

The Philippine Information Agency, in coordination with the NICA and the DICT shall ensure the effective information dissemination pursuant to this provision.

All LGUs and private organizations including the civil society organizations, private enterprises, and non-government organizations, civic, and people's organizations, are encouraged to observe National Cybersecurity Awareness Month in simple rites and participate in the activities.

SEC. 18. *The National Cybersecurity Plan.* – A National Cybersecurity Plan (NCSP) shall be formulated by the Philippine Cybersecurity Council to strengthen the country's institutional capacity to protect systems, networks, and programs from digital attacks and promote security and resilience of the Philippine cyberspace.

SEC. 19. *Critical Information Infrastructure (CII).* – This Act shall cover CIIs, whether in the public or private sector, including:

a. Banking and finance;
b. Broadcast media;
c. Emergency services and disaster response;
d. Energy;
e. Health;
f. Telecommunications;
g. Transportation (land, sea, air); and
h. Water.

An entity, whether public or private, that owns, operates, and maintains CII in the industries mentioned above, and as updated by the Department of Information and Communications Technology (DICT), shall be covered by this Act.

The DICT shall institute a consultation process to update the definition of a CII, the list of CII institutions, and the sector or industry covered as CII every three (3) years from the effectivity of this Act.

SEC. 20. *Adoption of Minimum Information Security Standards.* – All covered CII institutions shall adopt and implement adequate measures to protect their ICT systems and infrastructure, and respond to and recover from any information security incident, in compliance with existing laws, rules and regulations.

They are required to:

a) Adopt the Code of Practice stipulated in the Philippine National Standard (PNS) on ISO/IEC 27001 Information Security Management System (ISMS) (series of standards) and PNS ISO 22301 Security and resilience – Business continuity management systems (BCMS). They shall also adopt the ISO/IEC 27701 Privacy Information Management Systems, as applicable;
b) Submit to the DICT a copy of their formal certification as proof of adoption of the PNS ISO/IEC 27000 (series of standards), PNS ISO 22301, and ISO/IEC 27701, as applicable; and
c) Ensure that their certificates are up-to-date and shall submit the latest annual audit confirmation to the DICT.

In lieu of the submission of formal certification above, covered CII institutions shall subject themselves to an annual information security self-assessment using standards, such as but not limited to, the Center for Internet Security (CIS) Controls or the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, during the first quarter of each year. The concerned institution shall submit this self-declaration and attest to its validity to the DICT on or before the 31st of March. The self-declaration shall be signed off

by the respective head of the department directly in charge of the agency's information security systems.

Each CII institution shall adopt programs, guidelines, and written procedures for the implementation of its chosen information security standard, which shall be included in their annual submission.

The DICT shall have the authority to determine and update information security standards, and require CII institutions to comply with such standards, as it deems it necessary and appropriate.

Nothing in this Act shall prevent a government agency or a sector regulator from imposing additional or more stringent information security standards for compliance by industry players under its jurisdiction, as it deems necessary.

SEC. 21. *Prosecution of Cyber Offenders.* – The Department of Justice in coordination with the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall establish specialized units for the investigation and prosecution of cybercrime offenders.

The Department of Justice (DOJ) shall develop and implement guidelines for the swift prosecution of cybercrime offenses especially when the perpetrators are outside the Philippines, ensuring prosecution and imposition of appropriate penalties and sanctions in accordance with existing laws.

The government shall provide training for law enforcement officers, prosecutors, and judges on cybersecurity and cybercrime to ensure effective.

SEC. 22. *Penal Provisions.* – Any violation under Sections 10 and 11 of this Act, after due notice and hearing, shall be penalized with imprisonment of not less than six (6) months but not more than two (2) years or a fine of not more than One (1) million pesos, or both at the discretion of the court.

SEC. 23. *Appropriations.* – The amount of necessary to carry out its functions shall be included in the annual General Appropriations Act.

SEC. 24. *Implementing Rules and Regulations.* – The NICA and DICT, in consultation with relevant agencies, shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act.

SEC. 25. *Separability Clause.* – If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 26. *Repealing Clause.* – All laws, decrees, orders, rules and regulations or other issuances or parts thereof inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

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

Approved,