

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session



HOUSE BILL NO. 6090

Introduced by **REPRESENTATIVE AUDREY KAY T. ZUBIRI**

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

EXPLANATORY NOTE

In recent years, the Philippines has experienced an escalation in cyber incidents. Data from the Cybercrime Investigation and Coordinating Center (CICC) show complaints surged from 3,317 in 2023 to over 10,000 in 2024—a threefold increase—amounting to nearly PhP198 million in reported financial losses¹. Simultaneously, household level cyber incidents such as text scams, phishing, hacking, and cyberbullying rose sharply, affecting 62.5 percent of Filipinos with ICT devices in 2024, up from 31.1 percent in 2019.²

Corporate and institutional cybersecurity is similarly besieged. A survey from a cyber defense company reported that over 80 percent of Philippine organizations suffered an average of three cybersecurity breaches in 2024³. Meanwhile, the Philippines continues to rank among the world's top 10 countries in malware, phishing, and ransomware targeting⁴.

Despite these alarming trends, preparedness remains inadequate: only 6% of Philippine firms have reached a “mature” level in cybersecurity readiness. Around 85% experienced AI-

¹ <https://businessmirror.com.ph/2025/02/03/cybercrime-toll-%E2%82%B1198m-in-2024/>

² <https://www.bworldonline.com/the-nation/2025/07/21/686596/cybercrime-victims-in-phl-double-in-2024/>

³ [Philippines Organisations Impacted by Cyber Security... | BlueVoyant](#)

⁴ [The Cybersecurity Council Of The Philippines Is Launched](#)

related security incidents, and over half endured cyberattacks—yet investments in integrated cybersecurity infrastructure remain low⁵.

The proposed Cybersecurity Act seeks to institutionalize and strengthen the national cybersecurity framework through a comprehensive and coordinated approach. It establishes the Philippine Cybersecurity Council under the Office of the President to serve as the central authority for policy formulation, incident response, and inter-agency coordination. The bill mandates the enhancement of the Department of Information and Communications Technology's Cybersecurity Bureau, including 24/7 operations of the National Computer Emergency Response Team and the National Security Operations Center, to ensure real-time monitoring and response. It requires mandatory reporting of data breaches by government agencies and private entities, imposes accountability on internet service providers for malware and botnet mitigation, and introduces proactive vulnerability assessments for government and critical infrastructure assets.

Furthermore, the Act promotes public awareness through the declaration of October as National Cybersecurity Awareness Month, strengthens partnerships with digital platforms to combat misinformation, and enforces international security standards such as ISO/IEC 27001 and NIST for critical sectors. It also provides for specialized units within the Department of Justice, NBI, and PNP to investigate and prosecute cybercrime offenders, with penalties for non-compliance on breach reporting and ISP obligations.

By consolidating governance, operational readiness, legal accountability, and public education, this measure aims to protect the nation's digital ecosystem, safeguard critical infrastructure, and build resilience against evolving cyber threats. The passage of this bill is imperative to ensure a secure, reliable, and trusted cyberspace for all Filipinos.

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


AUDREY KAY T. ZUBIRI
Representative, 3rd District of Bukidnon

⁵ [85% of PH companies grappled with cyber threats in '24—Cisco](#)

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 6090

Introduced by **REPRESENTATIVE AUDREY KAY T. ZUBIRI**

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:

1 **SECTION 1. *Short Title.*** – This Act shall be known as the “Cybersecurity Act.”

2
3 **SEC. 2. *Declaration of Policy.*** - The State recognizes the vital role of communication
4 and information in nation building. The State also recognizes its inherent obligation to ensure
5 that personal data information and communications systems in the government and the private
6 sectors are secured and protected. Towards this end, the State shall provide Filipinos a secure,
7 reliable, and trusted cyberspace through the formulation and enforcement of effective
8 cybersecurity policies, and establishment of a governance framework that shall efficiently
9 coordinate government agencies and relevant sectors in the preparation of proactive, timely,
10 and appropriate response against cybersecurity threats.

11
12 **SEC. 3. *Definition of Terms.*** – For purposes of this Act, the following terms are defined
13 as follows:

- 14 a) **Botnet** or “**robot network**” refers to a network of computers infected by malware that
15 is under the control of a single attacking party;
- 16 b) **Critical infrastructure** refers to assets, systems, and networks, whether physical or
17 virtual, that are considered so vital that their destruction or disruption would have a
18 debilitating impact on national security, health and safety, or economic well-being of
19 citizens, or any combination thereof;

- 1 c) **Critical Information Infrastructure (CII)** refers to computer systems, ICT
2 information and communications technology (ICT) networks, and digital assets that
3 are necessary for the continuous operation and delivery of the country's critical
4 infrastructure services.
- 5 d) **CII institution** refers to a government agency or a private company that owns,
6 operates, controls, and/or maintains critical information infrastructure, and whose
7 operation is nationwide in scope and/or covers metropolitan centers, including Metro
8 Manila, Metro Cebu, Metro Davao, and, by 2025, Metro Cagayan de Oro, or as defined
9 and updated by the Department of Economy, Planning, and Development (DEPDev)
10 or the Philippine Statistics Authority (PSA).
- 11 e) **Cybersecurity** refers to the organization and collection of resources, processes, and
12 structures to preserve Confidentiality, Integrity, Availability, Non-Repudiation,
13 Authenticity, Privacy and Safety (CIANA-PS) in cyberspace;
- 14 f) **Cybersecurity governance** refers to the strategic approach that governs the
15 implementation and maintenance of cybersecurity measures, which are intended to
16 protect information and digital assets from cyber threats and unauthorized access;
- 17 g) **Cyberspace** refers to complex environment resulting from the interaction of people or
18 software and services on the internet by means of technology devices and networks
19 connected to it, which does not exist in any physical form;
- 20 h) **Distributed denial of service (DDoS) attack** refers to a variant of a denial of service
21 (DoS) attack that employs very large numbers of attacking computers to overwhelm
22 the target with bogus traffic;
- 23 i) **Internet of Things (IoT) botnets** refer to a network of compromised or infected
24 Internet of Things devices that can be remotely controlled by cybercriminals for
25 malicious purposes;
- 26 j) **Malware** refers a file or code, typically delivered over a network, that infects,
27 explores, steals or conducts virtually any behavior an attacker wants; and
- 28 k) **National Cybersecurity Plan** refers to the security policies, procedures, and controls
29 required to protect the country against threats and risk.
- 30

31 **SEC. 4. Philippine Cybersecurity Council.** - The Philippine Cybersecurity Council is
32 hereby established, which shall be an inter-agency body administratively attached to the Office
33 of the President. The Council shall be headed by the Director-General of the National
34 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.

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

3

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

10

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

17

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

23

24 ISPs are mandated to conduct effective countermeasures including the following:

25

- 26 a) Performing cybersecurity hygiene in their Customer Premise Equipment (CPE) such as
27 changing the CPE default password, disabling unused ports, and other hardening
28 measures for CPE;
- 29 b) Notifying those infected by malware and providing clear but concise instructions on
30 how to clean their devices; and
- 31 c) Complying with requests for quarantining network segments which are attempting a
32 distributed denial of service (DDoS) attack or identified as part of a command-and-
33 control structure of a ransomware, malware, or botnet.

1 **SEC. 12. *Threats and Baseline Assessments of Government Cyberspace Assets.*** - The
2 Council shall develop capability to automatically scan all government and critical information
3 infrastructure assets exposed in the internet for their vulnerabilities and provide a risk score to
4 these scanned threats. The scores and vulnerabilities scanned shall be kept confidentially and
5 shall be provided to the owners of the scanned cybersecurity assets. Owners of these
6 compromised assets shall report to the Council how vulnerabilities were mitigated. The
7 Council shall develop and/or acquire the necessary tools to ensure that the assessments are
8 stored and disseminated to all government agencies. Private security research shall be allowed
9 to report their own findings subject to the necessary guidelines that the Council shall issue for
10 responsible disclosure of vulnerabilities. Legal protection shall be provided to any security
11 researcher disclosing any vulnerability found in any cyberspace asset.

12
13 **SEC. 13. *National Cybersecurity Threat Database.*** - The Council shall develop a
14 national cybersecurity threat database, which shall be accessible to the public. The list of
15 threats shall be curated based on the category of the threat and the type of the threat based on
16 their common vulnerability scoring system (CVSS), category and type. The threat database
17 shall be updated regularly. The Council shall develop and maintain a website to inform the
18 public of the latest trends in cybersecurity and to issue advisories.

19
20 **SEC. 14. *Standards to Protect Inter-Domain Internet Protocol (IP) Routing***
21 ***Protocol.*** - The Council shall, in consultation with the NTC, DICT, DOST, and
22 telecommunications providers, adopt and implement standards for securing inter-domain
23 internet protocol (IP) routing protocol, particularly Border Gateway Protocol (BGP) to attain
24 national compliance for securing inter-domain routing.

25
26 **SEC. 15. *Partnership with Digital Online Platforms.*** - The Council shall initiate
27 robust and meaningful partnerships with digital online and social media platforms to create a
28 mutually acceptable protocol for reporting, correcting and mitigating misinformation, and
29 online harms in line with the need to regulate digital online platforms, including social media
30 platforms.

31
32 **SEC. 16. *Multi-Disciplinary Approach.*** - All government agencies, including LGUs,
33 are enjoined to improve and develop their own cybersecurity strategies, sub-plans, and teams
34 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 DICT, shall be covered by this Act.

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

4
5 **SEC. 20. *Adoption of Minimum Information Security Standards.*** - All covered CII
6 institutions shall adopt and implement adequate measures to protect their ICT systems and
7 infrastructure, and respond to and recover from any information security incident, in
8 compliance with existing laws, rules and regulations.

9
10 They are required to:

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

21
22 In lieu of the submission of formal certification above, covered CII institutions shall
23 subject themselves to an annual information security self- assessment using standards, such as
24 but not limited to, the Center for Internet Security (CIS) Controls or the National Institute of
25 Standards and Technology (NIST) Special Publication (SP) 800-53, during the first quarter of
26 each year. The concerned institution shall submit this self-declaration and attest to its validity
27 to the DICT on or before the 31st of March. The self-declaration shall be signed off by the
28 respective head of the department directly in charge of the agency's information security
29 systems.

30
31 Each CII institution shall adopt programs, guidelines, and written procedures for the
32 implementation of its chosen information security standard, which shall be included in their
33 annual submission.

1 The DICT shall have the authority to determine and update information security
2 standards, and require CII institutions to comply with such standards, as it deems it necessary
3 and appropriate.
4

5 Nothing in this Act shall prevent a government agency or a sector regulator from
6 imposing additional or more stringent information security standards for compliance by
7 industry players under its jurisdiction, as it deems necessary.
8

9 **SEC. 21. *Prosecution of Cyber Offenders.*** - The Department of Justice in coordination
10 with the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall
11 establish specialized units for the investigation and prosecution of cybercrime offenders.
12

13 The Department of Justice (DOJ) shall develop and implement guidelines for the swift
14 prosecution of cybercrime offenses especially when the perpetrators are outside the
15 Philippines, ensuring prosecution and imposition of appropriate penalties and sanctions in
16 accordance with existing laws.
17

18 The government shall provide training for law enforcement officers, prosecutors, and
19 judges on cybersecurity and cybercrime to ensure effective.
20

21 **SEC. 22. *Penal Provisions.*** - Any violation under Sections 10 and 11 of this Act, after
22 due notice and hearing, shall be penalized with imprisonment of not less than six (6) months
23 but not more than two (2) years or a fine of not more than One (1) million pesos, or both at the
24 discretion of the court.
25

26 **SEC. 23. *Appropriations.*** - The amount of necessary to carry out its functions shall be
27 included in the annual General Appropriations Act.
28

29 **SEC. 24. *Implementing Rules and Regulations.*** - The NICA and DICT, in consultation
30 with relevant agencies, shall jointly formulate the necessary rules and regulations within ninety
31 (90) days from approval of this Act.
32

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

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

4
5 **SEC. 27. *Effectivity.*** - This Act shall take effect fifteen (15) days after its publication
6 in the Official Gazette or in any two (2) newspapers of general circulation in the Philippines.

7
8 *Approved,*