

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

TWENTIETH CONGRESS
Second Regular Session

House Bill No. **11370**



INTRODUCED BY REPRESENTATIVES RALPH WENDEL P. TULFO
AND JOCELYN P. TULFO

AN ACT
ESTABLISHING THE PHILIPPINE CYBERSECURITY COUNCIL AND
ENHANCING THE NATIONAL CYBERSECURITY FRAMEWORK

EXPLANATORY NOTE

Article II, Section 24 of the 1987 Philippine Constitution recognizes the vital role of communication and information in nation-building. Communication services, such as the internet, serve as major tools in driving economic and social development by connecting people and industry linkages which contribute toward a cohesive and progressive nation.

However, the increasing reliance on digital systems and internet-based technologies has made cybersecurity a critical concern for national security, economic stability, and public safety. Government services, financial institutions, critical infrastructure, and private individuals are now more exposed to cyber threats such as hacking, data breaches, cyber fraud, and attacks on essential systems. As of 2025, data from the Bangko Sentral ng Pilipinas showed that identity theft, account takeover, and social engineering made up 76% of reported cyber fraud losses, followed by hacking at 13%, and card not present fraud at 8%. The figures reflect the growing shift toward scam-driven, human-centered attacks as digital financial services expand and

transactions move faster across interconnected platforms.¹ These threats, if left unaddressed, may disrupt public services, compromise sensitive information, and undermine public trust.

This bill aims to strengthen the Philippines' national cybersecurity framework by establishing a National Cybersecurity Council and enhancing the capabilities of the Department of Information and Communications Technology (DICT) and the Cybercrime Investigation and Coordinating Center (CICC). It also introduces the creation of a Public Cyber Complaint and Rapid Response Unit to assist citizens affected by cybercrimes, scams, or data breaches, and the establishment of a Cyber-Justice Assistance Desk to provide free legal support to victims of online abused and exploitation.

Moreover, this bill complements Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012", by strengthening institutional governance and coordination in cybersecurity beyond criminal prosecution, and by focusing on prevention, preparedness, and resilience. It also protects national interests, strengthen digital governance, and ensure that technological advancement contributes to a safe, secure, and sustainable digital future for the Philippines.

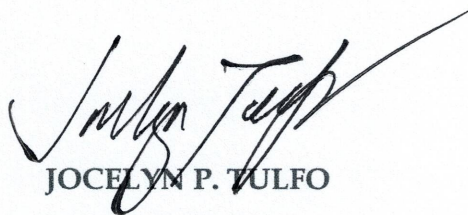
In view of the foregoing, the urgent passing of this bill is earnestly sought.



RALPH WENDEL P. TULFO

Representative

2nd District of Quezon City



JOCELYN P. TULFO

Representative

ACT-CIS Partylist

¹ Ta-Asan, Keisha, "Social engineering tops cyber threats in Philippines BSP study in 2025", *THE PHILIPPINE STAR*, 5 Feb 2026, <https://www.philstar.com/business/2026/02/05/2505751/social-engineering-tops-cyber-threats-philippines-bsp-study-2025>

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

TWENTIETH CONGRESS
Second Regular Session

House Bill No. **11370**

INTRODUCED BY REPRESENTATIVES RALPH WENDEL P. TULFO
AND JOCELYN P. TULFO

AN ACT
ESTABLISHING THE PHILIPPINE CYBERSECURITY COUNCIL AND
ENHANCING THE NATIONAL CYBERSECURITY FRAMEWORK

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

1 **SECTION 1. *Short Title.*** – National Cybersecurity Enhancement Act

2

3 **SEC. 2. *Declaration of Policy.*** – It is the policy of the State to protect the Filipino
4 people and the nation’s institution from all forms of cyber threats and attacks that
5 endanger public safety, privacy, and national security. The State recognizes that access
6 to safe and reliable cyberspace is a basic public right and a foundation of national
7 progress.

8

9 The State shall strengthen the country’s capability to prevent, detect, and
10 respond to cyber incidents by building a secure digital environment that upholds
11 transparency, accountability, and the protection of personal data. It shall ensure that
12 every Filipino, whether an individual user, worker, or business, is defended from
13 online abuse, fraud, exploitation, and misinformation.

1 To this end, the government shall institutionalize a unified national
2 cybersecurity framework that promotes cooperation among public and private
3 sectors, enhances digital resilience, and guarantees that technology serves the welfare
4 of the people and the integrity of the Republic.

5
6 **SEC. 3. *Creation of the National Cybersecurity Council.*** - There is hereby created a
7 National Cybersecurity Council, hereinafter referred to as the Council, which shall
8 serve as the primary policy-making, coordinating, and monitoring body on all matters
9 relating to cybersecurity, cyber-terrorism, and the protection of critical information
10 infrastructure in the Philippines.

11
12 The Council shall be attached to the Office of the President for policy direction
13 and oversight and shall be chaired by the Secretary of the Department of Information
14 and Communications Technology (DICT). The Executive Secretary and the Director-
15 General of the National Intelligence Coordinating Agency (NICA) shall serve as Co-
16 Chairpersons.

17
18 The Council shall be composed of the following members:

- 19
20 a. Secretary of the Department of Foreign Affairs (DFA);
21 b. Secretary of the Department of Science and Technology (DOST);
22 c. Secretary of the Department of the Interior and Local Government (DILG);
23 d. Secretary of the Department of Justice (DOJ);
24 e. Secretary of the Department of National Defense (DND);
25 f. Chairperson of the National Privacy Commission (NPC);
26 g. Commissioner of the National Telecommunications Commission (NTC);
27 h. Director of the National Bureau of Investigation (NBI);
28 i. Chief of the Philippine National Police (PNP); and
29 j. Executive Director of the Cybercrime Investigation and Coordinating
30 Center (CICC).

1
2 The Council shall coordinate closely with the Anti-Terrorism Council on
3 matters involving cyber-terrorism and digital threats to national security, ensuring
4 that preventive and investigate actions respect human rights and due process while
5 maintaining the safety of the public and the integrity of the State.

6
7 The Council may invite representatives from other public and private
8 institutions, including the business sector, academe, and civil society organizations,
9 to participate in meetings or consultations relevant to cybersecurity.

10
11 The DICT Cybersecurity Bureau shall serve as the Secretariat of the Council
12 and shall provide technical and administrative support necessary for the effective
13 performance of its functions.

14
15 **SEC. 4. Powers and Functions.** – The Council shall formulate and implement a
16 unified national cybersecurity policy and ensure the protection of the country's
17 information and communications technology systems, networks, and critical
18 information infrastructure. It shall serve as the center authority for coordinating
19 cybersecurity efforts across all government agencies and private institutions.

20
21 In pursuit of this mandate, the Council shall have the following powers and functions:

- 22
23 a. Policy Direction – Formulate, update, and oversee the National
24 Cybersecurity Plan and related strategies to strengthen digital resilience
25 and public protection;
26 b. Coordination and Monitoring – Coordinate all cybersecurity activities of
27 national government agencies, local government units, government-owned
28 or -controlled corporations, and private sector partners, and monitor
29 compliance with the national cybersecurity standards;

- 1 c. Cyber-Terrorism Prevention and Response – Coordinate with the Anti-
2 Terrorism Council (ATC) and relevant law enforcement and defense
3 agencies to prevent, detect, and respond to cyber-terrorism and digital
4 threats that endanger public safety or national security;
- 5 d. Incident Response – Oversee the establishment of a National Computer
6 Emergency Response Team (NCERT) and ensure the continuous operation
7 of the National Security Operations Center (NSOC) to respond to
8 cybersecurity incidents;
- 9 e. Capacity Building – Develop training, certification, and public education
10 programs to raise cybersecurity awareness and skill among government
11 employees, businesses and the general public;
- 12 f. Public Protection and Assistance – Establish a Public Cyber Complaint and
13 Rapid Response Unit and a Cyber-Justice Assistance Desk to provide
14 immediate help and free legal aid to citizens affected by cybercrimes, scams,
15 and online exploitation;
- 16 g. Partnership and International Cooperation – Strengthen coordination with
17 foreign governments, international organizations, and global cybersecurity
18 networks for information exchange and joint capacity-building initiatives;
- 19 h. Standards and Accreditation – Recommend minimum cybersecurity
20 standards, accreditation requirements, and risk-management protocols for
21 both public and private ICT systems handling sensitive or personal data;
22 and
- 23 i. Other Functions – Perform such other powers and duties as may be
24 necessary to fulfill its mandate under this Act and other existing laws.
25

26 **SEC. 5. *Meetings of the Council.*** – The Council shall meet at least once every
27 quarter to review the state of national cybersecurity, assess emerging threats, and
28 evaluate the implementation of ongoing programs and policies.
29

1 Special meetings may be convened by the Chairperson, or upon the written
2 request of any two (2) Co-Chairpersons, in cases of urgent cyber incidents, large-scale
3 data breaches, or threats to critical information infrastructure or national security. A
4 majority of all the members of the Council shall constitute a quorum. Decisions shall
5 be made by a majority vote of the members present. The council may create technical
6 working groups or subcommittees to focus on specific areas such as cyber-terrorism
7 prevention, data protection, financial security, or public complaint response. These
8 group shall submit their reports and recommendations to the Council for approval.

9
10 The Secretariat shall prepare the agenda, minutes, and documentation of all
11 meetings and shall ensure that summaries of non-classified actions and resolutions
12 are made available for public access, consistent with national security and data
13 privacy laws.

14
15 **SEC. 6. *Reporting of Cybersecurity Breaches.*** – All government agencies,
16 government-owned or -controlled corporations, and private entities operating critical
17 information infrastructure shall immediately report any cybersecurity breach,
18 incident, or data compromise to the National Cybersecurity Council, through the
19 Cybercrime Investigation and Coordinating Center and the National Computer
20 Emergency Response Team.

21
22 The initial report shall be made within twenty-four (24) hours from discovery
23 of the breach and shall include basic details necessary to assess the nature, scope, and
24 possible impact of the incident. A full report shall be submitted within seventy-two
25 (72) hours thereafter, unless otherwise extended by the Council for justifiable reasons.

26
27 Entities handling personal or sensitive information shall also notify affected
28 individuals and the NPC in accordance with the Data Privacy Act of 2012.

1 Failure to report a breach or the deliberate concealment of material information
2 shall constitute gross neglect and may result in administrative, civil, or criminal
3 liability under this Act and other applicable laws.

4
5 The Council shall maintain a confidential National Cyber Incident Registry for
6 classified data and a public advisory system that promptly informs citizens, without
7 disclosing sensitive details, of major threats or on-going attacks that could endanger
8 public welfare or essential services.

9
10 **SEC. 7. *Implementing Rules and Regulations.*** – The DICT, the DOJ, the DILG,
11 and the NSC shall jointly formulate the necessary rules and regulations within ninety
12 (90) days from approval of this Act, for its effective implementation.

13
14 **SEC. 8. *Separability Clause.*** – If any provision of this Act is hereby invalid, the
15 other provisions not affected shall remain in full force and effect.

16
17 **SEC. 9. *Repealing Clause.*** - All laws, decrees, orders, rules, and regulations or
18 other issuances or part thereof inconsistent with the provisions of this Act are hereby
19 repealed accordingly.

20
21 **SEC. 10. *Effectivity.*** – This Act shall take effect fifteen (15) days after its
22 publication in the Official Gazette or in any two (2) newspapers of general circulation
23 in the Philippines.

24
25 Approved,