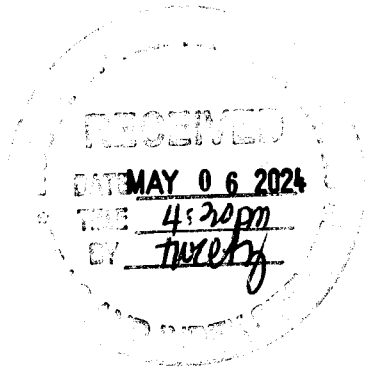
Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila



NINETEENTH CONGRESS
Second Regular Session

HOUSE BILL NO. 10355

Introduced by **Representative Jaime R. Fresnedi**

EXPLANATORY NOTE

The proposed "*Cybersecurity Act*" seeks to address the growing challenges posed by cyber threats in the Philippines by institutionalizing and strengthening the National Cybersecurity Council (NCC) as the primary authority responsible for cybersecurity matters. The measure provides for the renaming of the National Cybersecurity Inter-Agency Committee into the National Cybersecurity Council (NCC) with more defined powers and functions. It also provides for the mandatory reporting of data breaches by government institutions and government-owned and controlled corporations (GOCCs).

As information and communication technology continue to advance, so do the methods and scale of cyber attacks. Recognizing the critical importance of safeguarding cyberspace and ensuring data protection, the state must establish a robust cybersecurity framework that aligns with international standards all the while facilitating the flow of information by giving the NCC more powers and functions to ensure the security of the Philippine webspace and of it users.

Data on cyber attacks in the Philippines underscores the urgency of this measure. In recent years, the Philippines has experienced a significant increase in cyber attacks targeting government, public, and military networks, as well as private sector entities. In 2024, an unsuccessful hacking of various Philippine government websites and email systems was reported. This includes the Philippine Coast Guard, the Cabinet Secretary, the Department of Justice, the National Coast Watch System, DICT itself, and the "private" website of President Ferdinand Marcos Jr. Although the attempt proved to be unsuccessful, it only goes to show that threats will always persist and the country must remain proactive in fortifying its cyber defenses.

According to Kaspersky Security Network (KSN), the Philippines dropped to fourth place from fifth in the global ranking of countries most targeted by global threats. KSN also reported that web threats in the country in the year 2023 fell by 2%, however, we still remain as one of the top countries in Southeast Asia with the most online threats. The country also secured the 61st position among 194 countries in the International Telecommunication Union (ITU) Global Cybersecurity Index of 2020. Although it received commendable scores for its legal framework and collaborative efforts, the report underscored opportunities for enhancement in technical capabilities, organizational structure and capacity building initiatives.

In today's digital world where everything and everyone seems to be interconnected and where digital technologies permeate every aspect of our lives, complacency in cybersecurity measures is a luxury we cannot afford. The evolving nature of cyber threats demands vigilance and defense strategies. While advancements in technology bring unprecedented opportunities, they also present new ways for malicious individuals to exploit even the smallest vulnerability. By remaining vigilant, investing in robust cybersecurity frameworks and fostering a culture of awareness and accountability, we can mitigate risks and safeguard our digital ecosystems for the benefit of all.

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

JAIME R. FRESNEDI
Representative
Lone District, Muntinlupa City

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

NINETEENTH CONGRESS
Second Regular Session

HOUSE BILL NO. 10355

Introduced by **Rep. Jaime R. Fresnedi**

AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY INTER-AGENCY COMMITTEE CREATED UNDER EXECUTIVE ORDER NO. 95 (S. 2019), RENAMING IT TO NATIONAL CYBERSECURITY COUNCIL, 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 Act*".

Sec. 2. *Declaration of Policy.* – The state recognizes the importance of establishing a more secure cyberspace and a data protection regime that is compliant with international standards and ensures the free flow of information. Towards this end, it shall pursue measures to institutionalize and strengthen as well as enhance the protection of the nation's critical information structures especially government, public and military networks and infrastructure to ensure their continuous operations even during crises and emergencies.

Sec. 3. *Cybersecurity Council.* – The National Cybersecurity Inter-Agency Committee created under Executive Order No. 95 (s. 2019) is hereby institutionalized and renamed as the National Cybersecurity Council (NCC) under the administrative supervision of the Office of the President.

Sec. 4. *Reorganization of the Council.* – The Council shall be chaired by the Secretary of the Department of Information and Communications Technology (DICT) and co-chaired by the Executive Secretary and the National Security Adviser. It shall further be composed of the following 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); *and*
i) Governor of the *Bangko Sentral ng Pilipinas* (BSP) as members.

The National Cybersecurity Council shall have a secretariat to be headed by an Executive Director. The organizational structure and staffing pattern of the secretariat shall be formulated by the Secretary of the Department of Information and Communication Technology (DICT), subject to the approval of the Department of Budget and Management (DBM) in accordance with Executive Order No. 292, otherwise known as the "Administrative Code of 1987".

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

Sec. 5. *Powers and Functions.* – The National Cybersecurity Council shall be the main 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 digital and electronic documents and communications, following best practices. These protocols shall be updated periodically and as necessary.
d) Enhance 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 sure recommendations and such other reports as the president may from time to time direct; and
i) Perform such other functions as may be necessary.

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

Sec. 7. *Report of the Data Breach.* – Government institutions, agencies and instrumentalities, including government owned and controlled corporations are required to report to the National Cybersecurity 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.

Failure to make the required report shall be penalized with administrative sanctions in accordance with existing laws, rules and regulations.

Sec. 8. *Reportorial Requirement.* – The National Cybersecurity Council shall submit quarter a 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. The Council may request for an executive session from Congress if it may be deemed necessary.

Sec. 9. *Appropriations.* – The amount necessary to carry out its functions shall be included in the annual General Appropriations Act.

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

Sec. 11. *Repealing Clause.* – All laws, decrees, executive orders, proclamations, rules and regulations and other issuances or part or parts thereof, which are inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

Sec. 12. *Separability Clause.* – If for any reason, any provision of this Act is declared invalid or unconstitutional, the remaining provisions not affected thereby shall continue to be in force and effect.

Sec. 13. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in any two (2) newspapers of general circulation.

Approved,