

NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)



Senate
Office of the Secretary

'22 OCT -5 P5:50

SENATE
S.B. No. 1365

RECEIVED BY: _____

Introduced by **SENATOR IMEE R. MARCOS**

**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**

EXPLANATORY NOTE

Article 2, Section 5 of the Constitution provides that "the maintenance of peace and order, the protection of life, liberty and property and the promotion of the general welfare are essential for the enjoyment of the people of all the blessings of democracy." The evolution of Information Computer Technology (ICT) has brought tremendous advantages to the growth of our economy, as well as to the success of businesses in the country. Our countrymen, from all walks of life, are equally benefiting from the said advancement of technology. However, there is an urgent need to step-up and ensure the country's readiness against deliberate cyber-attacks which has become a serious national security threat.

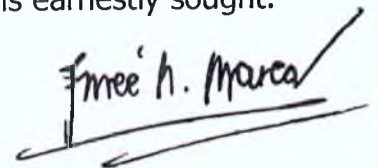
The International Telecommunications Union's 2021 Global Cybersecurity Index (GCI) ranked the Philippines 61st out of 194 countries in terms of commitment in adopting cybersecurity practices. In July 2022, Russian cybersecurity firm Kaspersky came up with a global ranking of countries with most online threats detected in 2021 where the Philippines moved up to 4th place from 5th in the past year. A total of 50,544,908 web threats were detected by Kaspersky in the Philippines in 2021 alone.

Kaspersky data further show that web threat attempts against Filipino users of Kaspersky software grew 432.75% from 9,487,775 in 2017 to 50,544,908 in 2021. With the pandemic-borne shift towards remote working, the overall cyber-attacks versus local businesses rose by 141% from 2019 (2,549,698) to 2021 (6,150,891). Yeo Siang Tiong, General Manager for Southeast Asia at Kaspersky, stated that "Cyber threats are here to stay as it is parallel with the digitalization drive in the Philippines."

In order to enhance our cybersecurity capabilities, this bill seeks to institutionalize and strengthen the National Cybersecurity Inter-Agency Committee (NCIAC) and empower it to be the main authority that will address all cybersecurity related matter. It shall assess the vulnerabilities and risks of the country's cybersecurity and issue updated protocols to all government employees for the proper handling, distribution and storage of all forms of documents and communications as well as to enhance public-private partnership in promoting cybersecurity.

The National Cybersecurity Inter-Agency Committee shall be transformed into a council with more powers and functions. It shall be reorganized by designating the Secretary of DICT as its Chairperson, adding other secretaries of government agencies as its members, and the appointing permanent personnel as its secretariat to be headed by an Executive Director in order to ensure its continuous and focused performance. Thus, it shall be renamed the "National Cybersecurity Council."

For the abovementioned reasons, the passage of this bill is earnestly sought.


IMEE R. MARCOS

NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

'22 OCT -5 P5 50

SENATE
S.B. No. 1365

RECEIVED BY: 

Introduced by **SENATOR IMEE R. MARCOS**

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 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 growth of information computer technology
4 is accompanied by new and serious threats and, as such, the state recognizes as vitally
5 important the establishment of a more secure cyberspace and a data protection regime
6 that is compliant with international standards and ensures the free flow of information.
7 Towards this end, there is a need to institutionalize and strengthen the National Inter-
8 Agency Cybersecurity Committee (NIAC) to enhance the protection of the nation's
9 critical information structures especially government, public and military networks and
10 infrastructure, ensuring their continuous operations even during crises and
11 emergencies

12
13 **SEC. 3. Cybersecurity Council.** – The National Cybersecurity Inter-Agency
14 Committee created under executive order no. 95 (s. 2019) is hereby institutionalized
15 and reorganized and rename it to National Cybersecurity Council (NCC) under the
16 administrative supervision of the Office the President.

17
18 **SEC. 4. Reorganization of the Council.** – The Council is chaired by the Secretary
19 of the Department of Information and Communications Technology (DICT) and co-
20 chaired by the Executive Secretary and the National Security Adviser and Director-

1 General of the National Security Council (NSC), and shall further be composed of the
2 following officials as members:

- 3
- 4 • Secretary of the Department of Foreign Affairs (DFA);
- 5 • Secretary of the Department of Finance (DOF);
- 6 • Secretary of the Department of Science and Technology (DOST);
- 7 • Secretary of the Department of Interior and Local Government (DILG);
- 8 • Secretary of the Department of Justice (DOJ);
- 9 • Secretary of the Department of Energy (DOE);
- 10 • Secretary of the Department of National Defense (DND);
- 11 • Secretary of the Department of Transportation (DOTr);
- 12 • Secretary of the Presidential Communication Operations Office (PCOO);
- 13 • Commissioner of the National Telecommunications Commission (NTC);
- 14 • Director-General of the National Intelligence Coordinating Agency (NICA);
- 15 • Director of the National Bureau of Investigation (NBI);
- 16 • Chief of the Philippine National Police (PNP);
- 17 • Chief of Staff of the Armed Forces of the Philippines;
- 18 • Chairman of the National Privacy Commission (NPC);
- 19 • Executive Director of the Anti-Terrorism Council-Program Management Center
20 (ATM-PMC);
- 21 • Executive Director of the Cybercrime Investigation and Coordinating Center
22 (CICC); and
- 23 • Governor of the *Bangko Sentral ng Pilipinas* (BSP) as members.
- 24

25 The National Cybersecurity Council shall have a secretariat to be headed by an
26 Executive Director. The organizational structure and staffing pattern of the secretariat
27 shall be formulated by the Secretary of the Department Information and
28 Communication Technology (DICT), subject to the approval of the Department of
29 Budget and Management (DBM) in accordance with executive order no. 292, otherwise
30 known as the "Administrative code of 1987".

31

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

35

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

1 **SEC. 5. Powers and Functions.** – The National Cybersecurity Council shall be the
2 main authority to exercise powers and functions that would address all cybersecurity
3 related matter. It shall perform the following functions:

- 4
- 5 a. Assess the vulnerabilities of the country's cybersecurity;
- 6
- 7 b. Capacity building for the purpose of responding to Cybersecurity threats and
8 emergencies;
- 9
- 10 c. Issue updated security protocols to all government employees in the storage,
11 handling and distribution of all forms (digital, electronic, snail mail, etc.) of
12 documents and communications, following best practices, these protocols shall
13 be updated periodically and, as necessary, in light of the rapid developments in
14 information and communications technology.
- 15
- 16 d. Enhance the public-private partnership in the field of information sharing involving
17 cyberattacks, threats and vulnerabilities to cyber threats;
- 18
- 19 e. Conduct periodic strategic planning and workshop activities that will reduce the
20 country's vulnerabilities to cyber threats;
- 21
- 22 f. Direct its member agencies and appropriate agencies to implement cybersecurity
23 measures as may be required by the situation;
- 24
- 25 g. Serve as the country's coordinating arm on domestic, international, and
26 transnational efforts pertaining to cybersecurity;
- 27
- 28 h. Make such recommendations and/or such other reports as the president may from
29 time to time direct; and
- 30
- 31 i. Perform such other functions as may be necessary.

32

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

36

37 **SEC. 7. Report of Data Breach.** – Government institutions, agencies,
38 instrumentalities, including government owned and controlled corporations, all private
39 corporations, companies and business establishments, operating wholly or partly in the
40 Philippines, are required to report to the National Cybersecurity Council, within a
41 reasonable period of time, all kinds of data breach occurring in their jurisdiction. The

1 Council shall conduct trainings on cybersecurity to all stakeholders for the effective
2 implementation of this proviso.

3
4 Failure to make the required report shall be penalized with imprisonment of not
5 less than six (6) months but not more than two (2) years or a fine of not more than
6 One (1) million pesos, or both at the discretion of the court. In case of penalty of
7 imprisonment, the same shall be imposed on the officials or persons who are
8 responsible to make the report to be determined in the Implementing Rules and
9 Regulations;

10
11 **SEC. 8. Reportorial Requirement.** – The National Cybersecurity Council shall
12 submit quarterly report, or as often as may be necessary, to the President of the
13 Philippines and to Congress on the state of cybersecurity threats and other related
14 information. The Council may request for an executive session from Congress if it may
15 deem necessary.

16
17 **SEC. 9. Appropriations.** – The amount of necessary to carry out its functions
18 shall be included in the annual General Appropriations Act.

19
20 **SEC. 10. Implementing Rules and Regulations.** – The DICT, the DOJ, the DILG
21 and the NSC shall jointly formulate the necessary rules and regulations within ninety
22 (90) days from approval of this Act, for its effective implementation.

23
24 **SEC. 11. Separability Clause.** – If any provision of this Act is held invalid, the
25 other provisions not affected shall remain in full force and effect.

26
27 **SEC. 12. Repealing Clause.** – All laws, decrees, orders, rules and regulations or
28 other issuances or parts thereof inconsistent with the provisions of this Act are hereby
29 repealed or modified accordingly.

30
31 **SEC. 15. Effectivity.** – This Act shall take effect fifteen (15) days after its
32 publication in the *Official Gazette* or in any two (2) newspapers of general circulation
33 in the Philippines.

Approved,