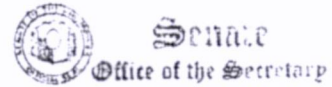


EIGHTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)



20 MAR -2 P5:34

SENATE

S. B. NO. 1388

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.

Reports show that the International Telecommunications Union's 2018 *Global Cybersecurity Index* (GCI) lists the Philippines as one of the countries with the lowest levels of cybersecurity. In August 2019, Russian cybersecurity firm Kaspersky came up with a report on global list of countries with most online threats detected in the 2nd quarter of 2019 where the Philippines moved up to 5th place from 9th a year earlier. Data from the company's security network showed that 37.4 percent, or seven

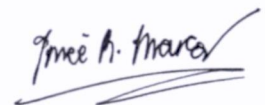
million, of Kaspersky's users in the Philippines were targets of a host of threats between April to May of 2019.

Some of the high-profile data leaks were the marketing server of the *Cebuana Lhuiller*, affecting more than 900,000 clients and the *Army First Scout Ranger Regiment's* website, exposing information about 20,000 soldiers. The COMELEC data leak incident on March 2016 was said to be one of the biggest leaks in Philippines government history.

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
Senator

20 MAR -2 P5 :34

SENATE

S.B. No. 1388

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 **SEC 2. Declaration of Policy.** -- The growth of information computer technology is
3 accompanied by new and serious threats and, as such, the state recognizes as vitally
4 important the establishment of a more secure cyberspace and a data protection
5 regime that is compliant with international standards and ensures the free flow of
6 information. Towards this end, there is a need to institutionalize and strengthen the
7 National Inter-Agency Cybersecurity Committee (NIAC) to enhance the protection of
8 the nation's critical information structures especially government, public and military
9 networks and infrastructure, ensuring their continuous operations even during crises
10 and emergencies.

11

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

1 **SEC. 4. Reorganization of the Council-** The Council is chaired by the Secretary of
2 the Department of Information and Communications Technology (DICT) and co-
3 chaired by the Executive Secretary and the National Security Adviser and Director-
4 General of the National Security Council (NSC), and shall further be composed of the
5 following officials as members:

- 6
- 7 • Secretary of the Department of Foreign Affairs (DFA);
- 8 • Secretary of the Department of Finance (DOF);
- 9 • Secretary of the Department of Science and Technology (DOST);
- 10 • Secretary of the Department of Interior and Local Government (DILG);
- 11 • Secretary of the Department of Justice (DOJ);
- 12 • Secretary of the Department of Energy (DOE);
- 13 • Secretary of the Department of National Defense (DND);
- 14 • Secretary of the Department of Transportation (DOTr);
- 15 • Secretary of the Presidential Communication Operations Office (PCOO);
- 16 • Commissioner of the National Telecommunications Commission (NTC);
- 17 • Director-General of the National Intelligence Coordinating Agency (NICA);
- 18 • Director of the National Bureau of Investigation (NBI);
- 19 • Chief of the Philippine National Police (PNP);
- 20 • Chief of Staff of the Armed Forces of the Philippines;
- 21 • Chairman of the National Privacy Commission (NPC);
- 22 • Executive Director of the Anti-Terrorism Council-Program Management Center
23 (ATM-PMC);
- 24 • Executive Director of the Cybercrime Investigation and Coordinating Center
25 (CICC); and
- 26 • Governor of the Bangko Sentral ng Pilipinas (BSP) as members.
- 27

28 The National Cybersecurity Council shall have a secretariat to be headed by an
29 Executive Director. The organizational structure and staffing pattern of the secretariat
30 shall be formulated by the Secretary of the Department Information and
31 Communication Technology (DICT), subject to the approval of the Department of

1 Budget and Management (DBM) in accordance with executive order no. 292, otherwise
2 known as the "administrative code of 1987.

3
4 The National Cybersecurity Council may invite concerned public and private agencies
5 or entities to participate, complement, and assist in the performance of its functions.

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

8
9 **SEC. 5. Powers and Functions**—The National Cybersecurity Council shall be the
10 main authority to exercise powers and functions that would address all
11 cybersecurity related matter. It shall perform the following functions:

- 12 a. Assess the vulnerabilities of the country's cybersecurity;
- 13 b. Capacity building for the purpose of responding to Cybersecurity threats and
14 emergencies;
- 15 c. Issue updated security protocols to all government employees in the
16 storage, handling and distribution of all forms (digital, electronic, snail mail,
17 etc.) of documents and communications. following best practices, these
18 protocols shall be updated periodically and, as necessary, in light of the
19 rapid developments in information and communications technology.
- 20 d. Enhance the public-private partnership in the field of information sharing
21 involving cyberattacks, threats and vulnerabilities to cyber threats;
- 22 e. Conduct periodic strategic planning and workshop activities that will reduce
23 the country's vulnerabilities to cyber threats;
- 24 f. Direct its member agencies and appropriate agencies to implement
25 cybersecurity measures as may be required by the situation;

- 1 g. Serve as the country's coordinating arm on domestic, international, and
2 transnational efforts pertaining to cybersecurity;
- 3 h. Make such recommendations and/or such other reports as the president
4 may from time to time direct; and
- 5 i. Perform such other functions as may be necessary.

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

9
10 **SEC. 7. Report of Data Breach**— Government institutions, agencies,
11 instrumentalities, including government owned and controlled corporations, all private
12 corporations, companies and business establishments, operating wholly or partly in
13 the Philippines, are required to report to the National Cybersecurity Council, within a
14 reasonable period of time, all kinds of data breach occurring in their jurisdiction. The
15 Council shall conduct trainings on cybersecurity to all stakeholders for the effective
16 implementation of this proviso.

17
18 Failure to make the required report shall be penalized with imprisonment of not less
19 than 6 months but not more than 2 years or a fine of not more than One (1) million
20 pesos, or both at the discretion of the court. In case of penalty of imprisonment, the
21 same shall be imposed on the officials or persons who are responsible to make the
22 report to be determined in the Implementing Rules and Regulations;

23
24 **SEC. 8. Reportorial Requirement**—The National Cybersecurity Council shall submit
25 quarterly report, or as often as may be necessary, to the President of the Philippines
26 and to Congress on the state of cybersecurity threats and other related information.
27 The Council may request for an executive session from Congress if it may deem
28 necessary.

1 **SEC. 9. Appropriations.** - The amount of necessary to carry out its functions shall
2 be included in the annual General Appropriations Act.

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

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

8 **SEC. 12. Repealing Clause.** - All laws, decrees or rules inconsistent with this Act
9 are hereby repealed or modified accordingly.

10 **SEC. 14. Effectivity.** - This Act shall take effect fifteen (15) days after the completion
11 of its publication in the *Official Gazette* or in at least two (2) newspapers of general
12 circulation.

Approved,