



MEMORANDUM

FOR : **The Directors**
Legal Affairs Service
Policy and Planning Service
Climate Change Service

All Bureau Directors

The Administrator
National Mapping Resource and Information Authority

The Chairman
Philippine Mining Development Corporation

The OIC Director
Environmental Law Enforcement and Protection Service

FROM : **The Director**
Legislative Liaison Office

SUBJECT : **INVITATION TO THE 2nd PUBLIC HEARING ON SENATE BILLS ON PHIVOLCS MODERNIZATION ACT, THE PHILIPPINE NUCLEAR REGULATION ACT, THE CRITICAL INFORMATION INFRASTRUCTURE PROTECTION ACT, AND THE SATELITE-BASED TECHNOLOGIES FOR INTERNET CONNECTIVITY ACT OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY OF THE SENATE OF THE PHILIPPINES**

DATE : 8 February 2024

In reference to the email received by our Office, the Committee on Science and Technology, joint with the Committees on Energy; Ways and Means; Public Service; and Finance of the Senate of the Philippines is inviting the Department to the **2nd Public Hearing on 12 February 2024, Monday, 11:30 AM, Senator Padilla Room, 2nd Floor, Senate of the Philippines, Pasay City**, to discuss the following legislative measures:

A. Phivolcs Modernization Act

1. **Senate Bill No. 2038**, "An Act Providing for the Modernization of the Philippine Volcanology and Seismology (PHIVOLCS), Providing Funds Therefor and for Other Purposes" (*Introduced by Sens. Zubiri, J., Villanueva, J., and Escudero, F.*)
2. **Senate Bill No. 2152**, "An Act Providing for the Modernization of the Philippine Volcanology and Seismology (PHIVOLCS), Providing Funds Therefor and for Other Purposes" (*Introduced by Sen. Jinggoy Estrada*)
3. **Senate Bill No. 2156**, "An Act Providing for the Modernization of the Philippine Volcanology and Seismology (PHIVOLCS), Providing Funds Therefor and for Other Purposes" (*Introduced by Sen. Ramon Bong Revilla, Jr.*)
4. **Senate Bill No. 2164**, "An Act Providing for the Modernization of the Philippine Volcanology and Seismology (PHIVOLCS), Providing Funds Therefor and for Other Purposes" (*Introduced by Sen. Francis Tolentino*)

B. Comprehensive Atomic Regulation/ Philippine Nuclear Regulation Act

1. **Senate Bill No. 1194**, "An Act Providing for a Comprehensive Nuclear Regulatory Framework, Creating for the Purpose, The Philippine Nuclear Regulatory Commission, and Appropriating Funds Therefor" (*Introduced by Sen. Francis Tolentino*)
2. **Senate Bill No. 1491**, "An Act Providing for a Comprehensive Atomic Regulatory Framework, Creating for the Purpose the Philippine Atomic Regulatory Commission, and Appropriating Funds Therefor" (*Introduced by Sen. Ramong Bong Revilla, Jr.*)
3. **Senate Bill No. 2498**, "AN ACT ESTABLISHING THE PHILIPPINE ATOMIC ENERGY REGULATORY AUTHORITY AND PROVIDING FOR A COMPREHENSIVE LEGAL FRAMEWORK FOR NUCLEAR SAFETY, SECURITY AND SAFEGUARDS IN THE PEACEFUL UTILIZATION OF NUCLEAR ENERGY IN THE PHILIPPINES AND APPROPRIATING FUNDS THEREFOR" (Introduced by Sen. Francis "Chiz" F. Escudero)
4. **House Bill No. 9293**, "AN ACT ESTABLISHING THE PHILIPPINE ATOMIC ENERGY REGULATORY AUTHORITY AND PROVIDING FOR A COMPREHENSIVE LEGAL FRAMEWORK FOR NUCLEAR" (Introduced by Representatives Cojuangco, Salceda, Macapagal-Arroyo, et al.)

C. Bills for Technical Working Group (TWG)

C1. Critical Information Infrastructure Protection Act

1. **Senate Bill No. 863**, "AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE" (*Introduced by Sen. Grace Poe*)
2. **Senate Bill No. 1382**, "AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE" (*Introduced by Sen. Juan Miguel "Migz" F. Zubiri*)
3. **Senate Bill No. 1701**, "AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE" (*Introduced by Sen. Raffy T. Tulfo*)
4. **Senate Bill No. 1923**, "AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE" (*Introduced by Sen. Ramon Bong Revilla, Jr.*)
5. **Senate Bill No. 2066**, "AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE" (*Introduced by Sen. Win Gatchalian*)

C2. Satellite-Based Technologies for Internet Connectivity Act

1. **Senate Bill No. 814**, "AN ACT ENCOURAGING AND PROMOTING THE USE AND DEVELOPMENT OF SATELLITE-BASED TECHNOLOGIES FOR INTERNET CONNECTIVITY" (*Introduced by Sen. Win Gatchalian*)
2. **Senate Bill No. 1380**, "AN ACT ENCOURAGING AND PROMOTING THE USE AND DEVELOPMENT OF SATELLITE-BASED TECHNOLOGIES FOR INTERNET CONNECTIVITY" (*Introduced by Sen. Juan Miguel "Migz" F. Zubiri*)

In this regard, may we respectfully request additional comments/recommendations on the abovementioned bills, as requested by the Committee. Kindly submit your comments on or **before 15 February 2024, 5:00 PM.** via email at denrilo@denr.gov.ph. Further, kindly inform us of the name/s of the representative/s from your office who will participate in the meeting so we may include him/her/them as resource person/s.

Attached herewith are the Letter Invitation and a copy of the bills for your reference.


ROMIROSE B. PADIN

cc: Undersecretary for Special Concerns and Legislative Affairs
Undersecretary for Finance, Information Systems and Climate Change



Republic of the Philippines
CONGRESS OF THE PHILIPPINES
Senate
Pasay City

COMMITTEE ON SCIENCE AND TECHNOLOGY

08 February 2024

HON. MARIA ANTONIA LOYZAGA

Secretary

Department of Environment and Natural Resources (DENR)

Dear Secretary Loyzaga:

Please be informed that the **Committee on Science and Technology**, joint with the Committees on Energy; Ways and Means; Public Services; and, Finance will conduct its **Second (2nd) Public Hearing** on **Monday, 12 February 2024, 11:30 a.m.** at the **Sen. Padilla Room, 2nd Floor, Senate of the Philippines.**

The Committee will continue to discuss the following legislative measures:

A. PHIVOLCS Modernization Act and Philippine Advanced Earthquake Monitoring and Early Warning System Act Of 2023

- **Senate Bill No. 2038**, "AN ACT PROVIDING FOR THE MODERNIZATION OF THE PHILIPPINE VOLCANOLOGY AND SEISMOLOGY (PHIVOLCS), PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES" (*Introduced by Sens. Zubiri, J., Villanueva, J., and Escudero, F.*)
- **Senate Bill No. 2152**, "AN ACT PROVIDING FOR THE MODERNIZATION OF THE PHILIPPINE VOLCANOLOGY AND SEISMOLOGY (PHIVOLCS), PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES" (*Introduced by Sen, Jinggoy Estrada*)
- **Senate Bill No. 2156**, "AN ACT PROVIDING FOR THE MODERNIZATION OF THE PHILIPPINE INSTITUTE OF VOLCANOLOGY AND SEISMOLOGY (PHIVOLCS), PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES" (*Introduced by Sen. Ramon Bong Revilla Jr.*)
- **Senate Bill No. 2164**, "AN ACT PROVIDING FOR THE MODERNIZATION OF THE PHILIPPINE INSTITUTE OF VOLCANOLOGY AND SEISMOLOGY (PHIVOLCS),

PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES” (*Introduced by Sen. Francis Tolentino*)

- **Senate Bill No. 2499**, “AN ACT PROVIDING FOR THE MODERNIZATION OF THE PHILIPPINE INSTITUTE OF VOLCANOLOGY AND SEISMOLOGY (PHIVOLCS), PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES” (*Introduced by Sen. Joseph Ejercito*)
- **Senate Bill No. 2316**, “AN ACT INSTITUTING A COMPREHENSIVE EARTHQUAKE MONITORING AND EARLY WARNING SYSTEM, APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES” (*Introduced by Sen. Mark A. Villar*)

B. Philippine National Nuclear Energy Safety Act

- **Senate Bill No. 1194**, AN ACT PROVIDING FOR A COMPREHENSIVE NUCLEAR REGULATORY FRAMEWORK, CREATING FOR THE PURPOSE, THE PHILIPPINE NUCLEAR REGULATORY COMMISSION, AND APPROPRIATING FUNDS THEREFOR (*Introduced by Sen. Francis Tolentino*)
- **Senate Bill No. 1491**, “AN ACT PROVIDING FOR A COMPREHENSIVE ATOMIC REGULATORY FRAMEWORK, CREATING FOR THE PURPOSE THE PHILIPPINE ATOMIC REGULATORY COMMISSION, AND APPROPRIATING FUNDS THEREFOR” (*Introduced by Sen. Ramon Bong Revilla, Jr.*)
- **Senate Bill No. 2498**, “AN ACT ESTABLISHING THE PHILIPPINE ATOMIC ENERGY REGULATORY AUTHORITY AND PROVIDING FOR A COMPREHENSIVE LEGAL FRAMEWORK FOR NUCLEAR SAFETY, SECURITY AND SAFEGUARDS IN THE PEACEFUL UTILIZATION OF NUCLEAR ENERGY IN THE PHILIPPINES AND APPROPRIATING FUNDS THEREFOR” (*Introduced by Sen. Francis “Chiz” F. Escudero*)
- **House Bill No. 9293**, “AN ACT ESTABLISHING THE PHILIPPINE ATOMIC ENERGY REGULATORY AUTHORITY AND PROVIDING FOR A COMPREHENSIVE LEGAL FRAMEWORK FOR NUCLEAR” (*Introduced by Representatives Cojuangco, Salceda, Macapagal-Arroyo, et al.*)

C. Bills for Technical Working Group (TWG)

C.1. Critical Information Infrastructure Protection Act

- **Senate Bill No. 863**, “AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE” (*Introduced by Sen. Grace Poe*)

- **Senate Bill No. 1382**, “AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE” *(Introduced by Sen. Juan Miguel “Migz” F. Zubiri)*
- **Senate Bill No. 1701**, “AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE” *(Introduced by Sen. Raffy T. Tulfo)*
- **Senate Bill No. 1923**, “AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE” *(Introduced by Sen. Ramon Bong Revilla, Jr.)*
- **Senate Bill No. 2066**, “AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE” *(Introduced by Sen. Win Gatchalian)*

C.2. Satellite-Based Technologies for Internet Connectivity Act

- **Senate Bill No. 814**, “AN ACT ENCOURAGING AND PROMOTING THE USE AND DEVELOPMENT OF SATELLITE-BASED TECHNOLOGIES FOR INTERNET CONNECTIVITY” *(Introduced by Sen. Win Gatchalian)*
- **Senate Bill No. 1380**, “AN ACT ENCOURAGING AND PROMOTING THE USE AND DEVELOPMENT OF SATELLITE-BASED TECHNOLOGIES FOR INTERNET CONNECTIVITY” *(Introduced by Sen. Juan Miguel “Migz” F. Zubiri)*

In this regard, may we invite you as a **Resource Person** to this meeting. Your **physical presence** is earnestly requested. The Committee would like to hear about your office’s informed opinion on the aforementioned legislative measures.

May we also request for your confirmation of availability. Should you be unable to attend the Public Hearing, may we respectfully request the names of your duly authorized representatives to speak on behalf of and for your office. Should you intend to make a presentation at the Public Hearing, the Committee would highly appreciate receiving a copy in advance. May we also respectfully request for a copy of your **position paper** on the above measures **on or before February 15, 2024**.

For any clarification on the matter, please feel free to contact the undersigned Committee Secretary at (02) 8552-6820, (02) 8552-6601 locals 3303, 3305 and 3306; or thru senatesciencetech@gmail.com.

Thank you very much.

For the Chairperson:


SEN. ALAN PETER "COMPAÑERO" S. CAYETANO


(MS.) JAMIE LYN DUQUE-DAILEG, MPP-NUS
Committee Secretary

22 OCT 12 P2:34

SENATE

Senate Bill No. 1382

RECEIVED BY: 

Introduced by **Senator JUAN MIGUEL F. ZUBIRI**

**AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO
ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS
AND INFRASTRUCTURE**

EXPLANATORY NOTE

The COVID-19 pandemic accelerated the country's digital transformation and digital economy. Filipinos now use 4.3 more new digital services on average compared to pre-pandemic years.¹ E-commerce grew significantly, and sales are expected to be valued at US\$10.3 billion by 2025.² The Bangko Sentral ng Pilipinas reported that 53% of adult Filipinos had electronic money accounts in 2021, up from 29% in 2019.³ According to the World Bank's assessment, online education and remote work are here to stay.⁴

Everyday life in our homes, corporate boardrooms, checkout counters of digital carts and government offices who deal with sundry items from food to frontline services and welfare payments or ayuda, among others need accuracy, speed and reliability. Breakneck speed is what we wish digital transactions would be. Yet, we know the promise of speed alone cannot engender trust. We must know that the system can be trusted because it is well-protected.

Increased use of digital technologies, especially the Internet, is accompanied by cyberthreats and risks. Malicious actors—from casual scammers to highly sophisticated state-backed groups—hunt for vulnerabilities in ICT systems and networks to steal information, disrupt essential services, and profit from attacks. Hence, it is critically important to ensure that the Philippines has a national policy framework for the protection of digital assets, especially critical information infrastructure (CII), against threats that could paralyze our economy and affect the wellbeing of Filipinos.

¹ Google, Temasek, & Bain & Company (2021). *e-Conomy SEA 2021: Roaring 20s: The SEA digital divide*. https://services.google.com/fh/files/misc/philippines_e_conomy_sea_2021_report.pdf

² GlobalData (9 Dec 2021). *Online shopping and rising internet penetration to lead Philippines e-commerce at 17% CAGR through 2025, forecasts GlobalData*. <https://www.globaldata.com/online-shopping-rising-internet-penetration-lead-philippines-e-commerce-17-cagr-2025-forecasts-globaldata/>

³ Villanueva, J. (24 Jan 2022). *PH digital transactions to grow despite challenges: BSP chief*. <https://www.pna.gov.ph/articles/1166236>; GCash alone grew 200% between 2020 and May 2022, now boasting 60 million users. See Cueto, F.E. (25 May 2022). *Gcash claims 60 million users in PH*. <https://www.manilatimes.net/2022/05/25/business/top-business/gcash-claims-60-million-users-in-ph/1844877>

⁴ World Bank (2020). *Building a resilient recovery. Philippines Economic Update: December 2020 edition*. <https://openknowledge.worldbank.org/bitstream/handle/10986/34829/Philippines-Economic-Update-Building-a-Resilient-Recovery.pdf>

The Philippine National Cyber Security Plan 2022 highlighted the goal of “assuring the continuous operation of the nation’s critical information infrastructure.” These digital systems underpin the operation of critical infrastructure, such as water, electricity, banking and financial networks, telecommunications, and other networks vital to the operation of the country.

In light of these risks, it is high time to ensure the protection of CIIs by ensuring, at the minimum, compliance with international standards and globally accepted best practices for cybersecurity.

As a proactive and institutionally cohesive response, this bill aims to protect the cybersecurity of CII by requiring the: (i) adoption of minimum information security standards, (ii) creation of a computer emergency response team and reporting of cybersecurity incidents, and (iii) development of a capable pool of cybersecurity professionals and practitioners that will be critical to the effective implementation of cybersecurity policy, rules, and standards.

If passed, the Critical Information Infrastructure Protection Act will provide a framework for ensuring the security and reliability of the country’s digital ecosystem, which is crucial to the country’s continued digitalization and growing digital economy. As a necessary step to improving Philippine cybersecurity, the passage of this bill is earnestly sought for the security and well-being of all Filipinos.



JUAN MIGUEL F. ZUBIRI

22 OCT 12 P2:34

SENATE

Senate Bill No. 1382

RECEIVED BY: 

Introduced by **Senator JUAN MIGUEL F. ZUBIRI**

**AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO
ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS
AND INFRASTRUCTURE**

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

1 **Section 1. Title.** – This Act shall be known as the “*Critical Information*
2 *Infrastructure Protection Act of 2022.*”
3

4 **Sec. 2. Declaration of Policy.** – The growth of information computer technology
5 is accompanied by new and serious threats and, as such, the state recognizes as vitally
6 important the establishment of a more secure cyberspace and a data protection regime
7 that is compliant with international standards and ensures the free flow of information.
8

9 It is the policy of the State to protect Critical Information Infrastructure (“CII”)
10 from cyberattacks and threats, data manipulation, cybercrimes, and activities of malicious
11 actors. The State recognizes that the protection of computers, networks, electronic
12 devices, and digital assets, including information, is a common objective and requires the
13 combined efforts of the public and private sectors, and cooperation with local and
14 international actors, in order to minimize the impact of, if not prevent, cyberattacks,
15 threats, and risks on the nation’s security and socio-economic well-being.
16

17 Further, the adoption and implementation of minimum information security
18 standards is a globally accepted best practice to provide guidance, which would lead to
19 more efficient use of resources, improved risk management, consistent delivery of critical
20 and essential services, and effective protection of the confidentiality, integrity, and
21 availability of information that is vital to the nation.
22

23 **Sec. 3. Definition.** – For the purpose of this Act and for the implementation of
24 the policy contained herein, the following definitions shall apply:
25

- 26 a. “Critical infrastructure” refers to assets, systems, and networks, whether
27 physical or virtual, that are considered so vital that their destruction or
28 disruption would have a debilitating impact on national security, health and
29 safety, or economic well-being of citizens, or any combination thereof.
30
31 b. “Critical Information Infrastructure (CII)” refers to computer systems, ICT
32 information and communications technology (ICT) networks, and digital assets

1 that are necessary for the continuous operation and delivery of the country's
2 critical infrastructure services.

- 3
- 4 c. "CII institution" refers to a government agency or a private company that owns,
5 operates, controls, and/or maintains critical information infrastructure, and
6 whose operation is nationwide in scope and/or covers metropolitan centers,
7 including Metro Manila, Metro Cebu, Metro Davao, and, by 2025, Metro
8 Cagayan de Oro, or as defined and updated by the National Economic
9 Development Authority (NEDA) or the Philippine Statistics Authority (PSA).
- 10
- 11 d. "Computer Emergency Response Team" or "CERT" refers to an organization
12 that studies computer and network security in order to provide incident
13 response services to victims of attacks, publish alerts concerning vulnerabilities
14 and threats, and to offer other information to help improve computer and
15 network security.
- 16
- 17 e. "Information security" refers to the preservation of the confidentiality, integrity,
18 and availability of information. This may also involve other properties, such as
19 authenticity, accountability, non-repudiation, and reliability of information.
- 20
- 21 f. "Information security incident" refers to an occurrence that actually or
22 potentially jeopardizes the confidentiality, integrity, or availability of an
23 information system or the information the system processes, stores, or
24 transmits or that constitutes a violation or imminent threat of violation of
25 security policies, security procedures, or acceptable use policies.
- 26
- 27 g. "Information system" refers to applications, services, information technology
28 assets, or any component handling information.
- 29

30 **Sec. 4. Coverage of Critical Information Infrastructure.** – This Act covers
31 CII, whether in the public or private sector, in industries including, but not limited to:

- 32
- 33 a. Banking and finance;
34 b. Broadcast media;
35 c. Emergency services and disaster response;
36 d. Energy;
37 e. Health;
38 f. Telecommunications;
39 g. Transportation (land, sea, air); and
40 h. Water.
- 41

42 An entity, whether public or private, that owns, operates, and maintains CII in the
43 industries mentioned above, and as updated by the Department of Information and
44 Communications Technology (DICT), shall be covered by this Act.

45

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

49

50 **Sec. 5. Adoption of Minimum Information Security Standards.** – All
51 covered CII institutions shall adopt and implement adequate measures to protect their
52 ICT systems and infrastructure, and respond to and recover from any information security
53 incident, in compliance with existing laws, rules and regulations.

54

1 They are required to:

- 2
- 3 a. adopt the Code of Practice stipulated in the Philippine National Standard (PNS)
4 on *ISO/IEC 27001 Information Security Management System (ISMS) (series of*
5 *standards)* and PNS *ISO 22301 Security and resilience – Business continuity*
6 *management systems (BCMS)*. They shall also adopt the *ISO/IEC 27701 Privacy*
7 *Information Management Systems*, as applicable;
- 8
- 9 b. submit to the DICT a copy of their formal certification as proof of adoption of
10 the PNS ISO/IEC 27000 (series of standards), PNS ISO 22301, and ISO/IEC
11 27701, as applicable; and
- 12
- 13 c. ensure that their certificates are up-to-date and shall submit the latest annual
14 audit confirmation to the DICT.
- 15

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

24

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

28

29 The DICT shall have the authority to determine and update information security
30 standards, and require CII institutions to comply with such standards, as it deems it
31 necessary and appropriate.

32

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

36

37 **Sec. 6. National Computer Emergency Response Team ("NCERT") as the**
38 **Centralized Information Security Incident Reporting Mechanism.** – All covered
39 CII Institutions shall:

40

- 41 a. report all information security incidents affecting their institutions to the DICT's
42 Philippine National Computer Emergency Response Team, which shall be the
43 central authority for all Sectoral and Organizational CERTs in the country;
- 44
- 45 b. submit an information security incident *detection* report to the NCERT within
46 twenty-four (24) hours upon detection of the incident(s). The report shall
47 contain basic information about the incident, such as: (1) date when the
48 incident was first detected, (ii) nature of the information security incident, (iii)
49 possible business processes and functions compromised, and (iv) agency's
50 initial response and next steps;
- 51
- 52 c. submit an incident *progress* report, upon request of the NCERT, in order to
53 help assess and provide the necessary support in responding to an incident;
- 54

- 1 d. submit a *post-incident* report, which contains the following information: (i)
2 magnitude of business operations compromised, (ii) risk assessment, and (iii)
3 the agency's response. They shall also provide the necessary additional
4 information about the incident, as requested by the NCERT;
5
6 e. compile on an annual basis a summary of all information security incident
7 reports and submit an annual report to the DICT Cybersecurity Bureau every
8 30th of June;
9
10 f. comply with the reporting mechanism and template prescribed by the DICT, in
11 the submission of all the reporting requirements described above: *Provided*,
12 that information-sharing shall be done using established communication
13 protocol, using at the minimum, the Traffic Light Protocol (TLP) as established
14 by the DICT MC 2017-005 or succeeding policies; and
15
16 g. participate in activities that help promote awareness, capacity building, and
17 improve an organization's information security readiness, protection, and
18 incident response capabilities, such as but not limited to cyber drills.
19

20 **Sec. 7. Designation of Personnel with Information Security Credentials.**

21 – All government agencies shall have at least one personnel with sufficient information
22 security training and credentials. Such personnel shall, preferably, hold at least Division
23 Chief plantilla position (or equivalent) and perform decision making or management
24 functions. The DICT shall identify and release a list of credentials that meet this
25 requirement. Such personnel shall be the point person for (i) compliance with prescribed
26 standards, (ii) building information security capability within the agency, and (iii)
27 compliance with the agency's and NCERT's reporting requirements.
28

29 **Section 8. Compliance by all covered CII Institutions.**

- 30
31 a. Government compliance: The Department of Budget and Management (DBM)
32 shall review the submission by a CII Institution to the DICT of a formal
33 certification or self-declaration of compliance with any of the prescribed
34 information security standards, whichever submission applies, as a prerequisite
35 to budgetary approval. A government institution or sector regulator, which
36 itself operates or has jurisdiction over CII, shall comply with the requirements
37 set forth in this Act.
38
39 b. Non-government or private company compliance: Compliance with this Act,
40 specifically of Sections 5 (standards) and 6 (reporting), shall be a prerequisite
41 for the granting of any regulatory approval, permit, and/or license to a private
42 company covered under Section 4 of this Act.
43

44 **Sec. 9. Implementing Agency.** – The DICT, through its Cybersecurity Bureau,
45 shall be the implementing agency of this Act, in accordance with the National
46 Cybersecurity Plan and relevant DICT policies. The DICT shall:
47

- 48 a. create and maintain a database of all certifications, self-declaration, and
49 attestations of all covered CII institutions;
50
51 b. prescribe minimum information security standards for compliance by all CII
52 institutions;
53
54 c. serve as the custodian for information security standards and incident reports;

- 1
2 d. collect and analyze all pertinent information about an information security
3 incident, and provide to government institutions, sectoral CERTs, and to the
4 public a technical report of information security incidents for purposes of policy,
5 regulation, and providing guidance to all stakeholders on local information
6 security issues.
7
8 e. prescribe a mechanism and template for the reporting of information security
9 incidents to the NCERT; and
10
11 f. institute a consultation process and hold consultations to update the coverage
12 and definition of CII, minimum information security standards, and recognize
13 individual information security certifications every three (3) years from the
14 effectivity of this Act.
15

16 **Sec. 10. – Responsibilities of the Department Heads and Sector**
17 **Regulators with jurisdiction over CII Institutions.** The heads of departments and
18 sector regulators who have a mandate over covered CII Institutions, including Sectoral
19 CERT Leads as identified in DICT DC 003-2020, in coordination with the DICT, shall be
20 responsible for issuing the necessary policy and regulation that promote information
21 security and require compliance of CII institutions with the prevailing standards to ensure
22 information security and business continuity.
23

24 **Sec. 11. Funding.** – The initial funding requirements for the implementation of
25 this Act shall be charged against the existing budget of the covered CII institutions and
26 such other appropriate funding sources as the DBM may identify, subject to relevant laws,
27 rules, and regulations.
28

29 **Sec. 12. Penalty.** – Non-compliance with the provisions of this Act, whether or
30 not it results in data loss, breaches, hacking, or similar incidents, may result in
31 administrative, civil, or criminal liability under applicable laws, including but not limited to
32 Republic Act No. 10175 also known as the Cybercrime Prevention Act of 2012 and
33 Republic Act No. 10173 or the Data Privacy Act of 2012.
34

35 **Sec. 13. Annual Report.** – Every 30th of April of every year, the DICT shall report
36 to the Office of the President the status of the implementation of this Act.
37

38 **Sec. 14. Separability Clause.** – If any provision of this Act is declared invalid or
39 unconstitutional, the remaining provisions not affected thereby shall continue to be in full
40 force and effect.
41

42 **Sec. 15. Repealing Clause.** – All laws, rules, and regulations inconsistent with
43 this Act are hereby repealed or modified accordingly.
44

45 **Sec. 16. Effectivity.** – This Act shall take effect fifteen (15) days after its
46 publication in the Official Gazette or in a newspaper of general circulation.

Approved,

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

23 JAN 18 P5 24

SENATE
S. No. 1701

RECEIVED BY: 

Introduced by **Senator Raffy T. Tulfo**

**AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE
INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO
PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY
(ICT) SYSTEMS AND INFRASTRUCTURE**

EXPLANATORY NOTE


The COVID-19 pandemic accelerated digitalization and expanded the country's digital economy. In comparison to pre-pandemic years, Filipinos now use 4.3 more new digital services on average. The increased use of digital technologies, particularly the Internet, is, however, accompanied by cyber threats and risks.

The "Critical Information Infrastructure Protection Act" (CIIPA) required the adoption of minimum information security standards, reporting and responding to cybersecurity incidents, and designating personnel with cybersecurity credentials, among other things, to protect the cybersecurity of critical infrastructure.

The CIIPA bill establishes a framework for ensuring the security and reliability of the country's digital ecosystem, which is critical to achieving the new administration's goal of safe, seamless, and reliable digitalization and connectivity for all.

Malicious actors—from casual scammers to highly sophisticated state-backed groups—hunt for vulnerabilities in ICT systems and networks to steal information, disrupt essential services, and profit from attacks. Recent studies ranked the Philippines fourth worldwide with the most number of web threats ¹and third most extorted by ransomware². Continued vulnerability to data breaches could cost an average of PHP 250 million³, for which the e-commerce, banking, and health sectors have become the top targets for cyberattacks. Hence, it is urgent for the Philippines to have a national policy framework for the protection of digital assets, especially critical information infrastructure (CII).

The passage of this measure is earnestly sought.



Raffy T. Tulfo
Senator

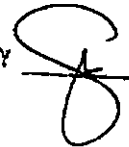
¹ <https://mb.com.ph/2022/07/11/kaspersky-philippines-ranked-4th-worldwide-with-most-number-of-web-threats/>

² <https://mb.com.ph/2022/07/11/kaspersky-philippines-ranked-4th-worldwide-with-most-number-of-web-threats/>

³ Based on the "Cost of Data Breaches Report 2022" converted from the global average of \$4.4 million. <https://www.darkreading.com/risk/most-companies-pass-on-breach-costs-to-customers>

23 JAN 18 P5:24

SENATE
S. No. 1701

RECEIVED BY 

Introduced by **Senator Raffy T. Tulfo**

**AN ACT REQUIRING CRITICAL INFORMATION INFRASTRUCTURE
INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO
PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY
(ICT) SYSTEMS AND INFRASTRUCTURE**

*Be it enacted by the Senate and House of Representatives of the Philippines in
Congress Assembled:*

1 Section 1. Title. – This Act shall be known as the "*Critical Information*
2 *Infrastructure Protection Act of 2022.*"

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
6 regime that is compliant with international standards and ensures the free flow of
7 information.

8 It is the policy of the State to protect Critical Information Infrastructure ("CII")
9 from cyberattacks and threats, data manipulation, cybercrimes, and activities of
10 malicious actors. The State recognizes that the protection of computers, networks,
11 electronic devices, and digital assets, including information, is a common objective
12 and requires the combined efforts of the public and private sectors, and cooperation
13 with local and international actors, in order to minimize the impact of, if not prevent,
14 cyberattacks, threats, and risks on the nation's security and socio-economic well-
15 being.

1 Further, the adoption and implementation of minimum information security
2 standards is a globally accepted best practice to provide guidance, which would lead
3 to more efficient use of resources, improved risk management, consistent delivery of
4 critical and essential services, and effective protection of the confidentiality, integrity,
5 and availability of information that is vital to the nation.

6 Sec. 3. Definition. – For the purpose of this Act and for the implementation of
7 the policy contained herein, the following definitions shall apply:

- 8
- 9 a. "Critical infrastructure" refers to assets, systems, and networks, whether
10 physical or virtual, that are considered so vital that their destruction or
11 disruption would have a debilitating impact on national security, health and
12 safety, or economic well-being of citizens, or any combination thereof.
- 13
- 14 b. "Critical Information Infrastructure (CII)" refers to computer systems, ICT
15 information and communications technology (ICT) networks, and digital
16 assets that are necessary for the continuous operation and delivery of the
17 country's critical infrastructure services.
- 18
- 19 c. "CII institution" refers to a government agency or a private company that
20 owns, operates, controls, and/or maintains critical information
21 infrastructure, and whose operation is nationwide in scope and/or covers
22 metropolitan centers, including Metro Manila, Metro Cebu, Metro Davao,
23 and, by 2025, Metro Cagayan de Oro, or as defined and updated by the
24 National Economic Development Authority (NEDA) or the Philippine
25 Statistics Authority (PSA).
- 26
- 27 d. "Computer Emergency Response Team" or "CERT" refers to an organization
28 that studies computer and network security in order to provide incident
29 response services to victims of attacks, publish alerts concerning
30 vulnerabilities and threats, and to offer other information to help improve
31 computer and network security.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

- e. "Information security" refers to the preservation of the confidentiality, integrity, and availability of information. This may also involve other properties, such as authenticity, accountability, non-repudiation, and reliability of information.

- f. "Information security incident" refers to an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

- g. "Information system" refers to applications, services, information technology assets, or any component handling information.

Sec. 4. Coverage of Critical Information Infrastructure. – This Act covers CII, whether in the public or private sector, in industries including, but not limited to:

- 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 Department of Information and Communications Technology (DICT), shall be covered by this Act.

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

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

9
10 They are required to:

- 11
- 12 a. adopt the Code of Practice stipulated in the Philippine National Standard
13 (PNS) on *ISO/IEC 27001 Information Security Management System (ISMS)*
14 *(series of standards)* and PNS *ISO 22301 Security and resilience – Business*
15 *continuity management systems (BCMS)*. They shall also adopt the *ISO/IEC*
16 *27701 Privacy Information Management Systems*, as applicable;
 - 17
 - 18 b. submit to the DICT a copy of their formal certification as proof of adoption
19 of the PNS ISO/IEC 27000 (series of standards), PNS ISO 22301, and
20 ISO/IEC 27701, as applicable; and
 - 21
 - 22 c. ensure that their certificates are up-to-date and shall submit the latest
23 annual audit confirmation to the DICT.

24

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

1 The self-declaration shall be signed off by the respective head of the department
2 directly in charge of the agency's information security systems.

3
4 Each CII institution shall adopt programs, guidelines, and written procedures
5 for the implementation of its chosen information security standard, which shall be
6 included in their annual submission.

7
8 The DICT shall have the authority to determine and update information security
9 standards, and require CII institutions to comply with such standards, as it deems it
10 necessary and appropriate.

11
12 Nothing in this Act shall prevent a government agency or a sector regulator
13 from imposing additional or more stringent information security standards for
14 compliance by industry players under its jurisdiction, as it deems necessary.

15
16 Sec. 6. National Computer Emergency Response Team ("NCERT") as the
17 Centralized Information Security Incident Reporting Mechanism. – All covered CII
18 Institutions shall:

- 19
20 a. report all information security incidents affecting their institutions to the
21 DICT's Philippine National Computer Emergency Response Team, which
22 shall be the central authority for all Sectoral and Organizational CERTs in
23 the country;
- 24
25 b. submit an information security incident *detection* report to the NCERT within
26 twenty-four (24) hours upon detection of the incident(s). The report shall
27 contain basic information about the incident, such as: (1) date when the
28 incident was first detected, (ii) nature of the information security incident,
29 (iii) possible business processes and functions compromised, and (iv)
30 agency's initial response and next steps;

- 1 c. submit an incident *progress* report, upon request of the NCERT, in order to
2 help assess and provide the necessary support in responding to an incident;
3
- 4 d. submit a *post-incident* report, which contains the following information: (i)
5 magnitude of business operations compromised, (ii) risk assessment, and
6 (iii) the agency's response. They shall also provide the necessary additional
7 information about the incident, as requested by the NCERT;
8
- 9 e. compile on an annual basis a summary of all information security incident
10 reports and submit an annual report to the DICT Cybersecurity Bureau every
11 30th of June;
12
- 13 f. comply with the reporting mechanism and template prescribed by the DICT,
14 in the submission of all the reporting requirements described above:
15 *Provided*, that information-sharing shall be done using established
16 communication protocol, using at the minimum, the Traffic Light Protocol
17 (TLP) as established by the DICT MC 2017-005 or succeeding policies.
18
- 19 g. participate in activities that help promote awareness, capacity building, and
20 improve an organization's information security readiness, protection, and
21 incident response capabilities, such as but not limited to cyber drills.
22

23 **Sec. 7. Designation of Personnel with Information Security Credentials.** – All
24 government agencies shall have at least one personnel with sufficient information
25 security training and credentials. Such personnel shall, preferably, hold at least
26 Division Chief plantilla position (or equivalent) and perform decision making or
27 management functions. The DICT shall identify and release a list of credentials that
28 meet this requirement. Such personnel shall be the point person for (i) compliance
29 with prescribed standards, (ii) building information security capability within the
30 agency, and (iii) compliance with the agency's and NCERT's reporting requirements.
31

1 **Sec. 8. Compliance by all covered CII Institutions.**

2
3 **a. Government compliance: The Department of Budget and Management**
4 **(DBM) shall review the submission by a CII Institution to the DICT of a**
5 **formal certification or self-declaration of compliance with any of the**
6 **prescribed information security standards, whichever submission applies, as**
7 **a prerequisite to budgetary approval. A government institution or sector**
8 **regulator, which itself operates or has jurisdiction over CII, shall comply**
9 **with the requirements set forth in this Act.**

10
11 **b. Non-government or private company compliance: Compliance with this Act,**
12 **specifically of Sections 5 (standards) and 6 (reporting), shall be a**
13 **prerequisite for the granting of any regulatory approval, permit, and/or**
14 **license to a private company covered under Section 4 of this Act.**

15
16 **Sec. 9. Implementing Agency. – The DICT, through its Cybersecurity Bureau,**
17 **shall be the implementing agency of this Act, in accordance with the National**
18 **Cybersecurity Plan and relevant DICT policies. The DICT shall:**

19
20 **a. create and maintain a database of all certifications, self-declaration, and**
21 **attestations of all covered CII institutions;**

22
23 **b. prescribe minimum information security standards for compliance by all CII**
24 **institutions;**

25
26 **c. serve as the custodian for information security standards and incident**
27 **reports;**

28
29 **d. collect and analyze all pertinent information about an information security**
30 **incident, and provide to government institutions, sectoral CERTs, and to the**
31 **public a technical report of information security incidents for purposes of**

1 policy, regulation, and providing guidance to all stakeholders on local
2 information security issues.

3
4 e. prescribe a mechanism and template for the reporting of information
5 security incidents to the NCERT; and

6
7 f. institute a consultation process and hold consultations to update the
8 coverage and definition of CII, minimum information security standards, and
9 recognize individual information security certifications every three (3) years
10 from the effectivity of this Act.

11
12 Sec. 10. – Responsibilities of the Department Heads and Sector Regulators with
13 jurisdiction over CII Institutions. The heads of departments and sector regulators who
14 have a mandate over covered CII Institutions, including Sectoral CERT Leads as
15 identified in DICT DC 003-2020, in coordination with the DICT, shall be responsible
16 for issuing the necessary policy and regulation that promote information security and
17 require compliance of CII institutions to the prevailing standards to ensure information
18 security and business continuity.

19
20 Sec. 11. Administrative Liability. – The respective heads of departments,
21 agencies, bureaus, offices, GOCCs, GFIs, and SUCs shall be administratively liable for
22 non-compliance with this Act pursuant to existing laws, rules, and regulations.

23
24 Sec. 12. Funding. – The initial funding requirements for the implementation of
25 this Act shall be charged against the existing budget of the covered CII institutions
26 and such other appropriate funding sources as the DBM may identify, subject to
27 relevant laws, rules, and regulations.

28
29 Sec. 13. Penalty. – Non-compliance with the provisions of this Act, whether or
30 not it results in data loss, breaches, hacking, or similar incidents, may result in
31 administrative, civil, or criminal liability under applicable laws, including but not limited

1 to Republic Act No. 10175 also known as the Cybercrime Prevention Act of 2012 and
2 Republic Act No. 10173 or the Data Privacy Act of 2012.

3
4 Sec. 14. Annual Report. – Every 30th of April of every year, the DICT shall report
5 to the Office of the President the status of the implementation of this Act.

6
7 Sec. 15. Separability Clause. – If any provision of this Act is declared invalid or
8 unconstitutional, the remaining provisions not affected thereby shall continue to be in
9 full force and effect.

10
11 Sec. 16. Repealing Clause. – All laws, rules, and regulations inconsistent with
12 this Act are hereby repealed or modified accordingly.

13
14 Sec. 17. Effectivity. – This Act shall take effect fifteen (15) days following the
15 completion of its publication in two (2) newspapers of general circulation.


Approved.

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



23 FEB 27 P2:10

SENATE
S. No. 1923

RECEIVED 

Introduced by SENATOR RAMON BONG REVILLA, JR.

AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS
TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND
INFRASTRUCTURE

EXPLANATORY NOTE

The latest Digital 2022 report of social media management firm Hootsuite and creative agency We Are Social revealed that internet users in the Philippines from ages 16 to 64 spend an average of 10 hours and 27 minutes on the internet per day. The same report showed that Filipino internet users enjoy activities online, such as watching educational videos, streaming TV content, listening to podcasts, playing video games, while others maximize online surfing for investment, insurance applications, and online banking each week¹.

In a country like ours where people are heavily reliant online, response to everyday needs will most likely evolve using technology and the internet. The exponential proliferation of E-commerce paved the way to accelerated use of information and communications technology (ICT) in critical infrastructure (CI). Unfortunately, our country has limited data protection mechanisms in place – making us enormously susceptible to various cybersecurity threats and risks.

Cyberattacks worldwide has already taken a toll to several countries' operation of CI – such as water, electricity, banking and financial networks, telecommunications, and other networks. In 2020, a cyber-attack in a German hospital caused disruption in the operations of its emergency facility – triggering the death of a patient being

¹ *Social media, internet craze keep PH on top 2 of world list* (April 29, 2022). Data accessed on 22 November 2022, from <https://newsinfo.inquirer.net/1589845/social-media-internet-craze-keep-ph-on-top-2-of-world-list/ixzz7alibO2QMW>

transported to another hospital 32 kilometers away which resulted to her death². Just last year in Ukraine, the war shifted to cyberspace as their government and critical infrastructure were bombarded with cyber-attacks. Since cyber criminals are increasingly targeting critical information infrastructure (CII), it is said that in the years to come, cyberspace will inevitably be exploited more by criminals, terrorists, and even governments to push their agenda³.

Cyberattacks on CI evidently opens debilitating effects on national security, health and safety, and economy of any country. Admittedly, the Philippines lacks a national policy directive requiring CI agencies to comply with standards, adopt measures to ensure information security of ICT networks and systems.

Owing to this unfortunate risks exposure, it is but urgent for Congress to pass a law that comprehensively adopts and implements minimum information security standards to improve risk management and effectively protect the confidentiality, integrity, and availability of information that is vital to our nation.

This proposed measure seeks to safeguard the cybersecurity of CII primarily through the adoption of minimum information security standards, and adherence to globally accepted best practices for cybersecurity. Moreover, this bill addresses our country's need for a national policy framework for the protection of digital assets, especially CII, against serious cyberthreats. The same move is considered crucial to the Philippines' continued digitalization and growing digital economy.

In view of the foregoing, the immediate approval of this bill is earnestly requested.



RAMON BONG REVILLA, JR.


² *Cybersecurity standards and a country's cyber resilience* (July 13, 2022). Data accessed on 28 November 2022, from <https://www.computex.ph/2022/07/cybersecurity-standards-and-a-country-s-cyber-resilience/>

³ *Ibid.*

23 FEB 27 P2:10

SENATE
S. No. 1923

RECEIVED


Introduced by SENATOR RAMON BONG REVILLA, JR.

AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS
TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND
INFRASTRUCTURE

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

1 Section 1. Title. – This Act shall be known as the "*Critical Information*
2 *Infrastructure Protection Act of 2023.*"

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
6 regime that is compliant with international standards and ensures the free flow of
7 information.

8 It is the policy of the State to protect Critical Information Infrastructure ("CII")
9 from cyberattacks and threats, data manipulation, cybercrimes, and activities of
10 malicious actors. The State recognizes that the protection of computers, networks,
11 electronic devices, and digital assets, including information, is a common objective
12 and requires the combined efforts of the public and private sectors, and cooperation
13 with local and international actors, in order to minimize the impact of, if not prevent,
14 cyberattacks, threats, and risks on the nation's security and socio-economic well-
15 being.

1 Further, the adoption and implementation of minimum information security
2 standards is a globally accepted best practice to provide guidance, which would lead
3 to more efficient use of resources, improved risk management, consistent delivery of
4 critical and essential services, and effective protection of the confidentiality, integrity,
5 and availability of information that is vital to the nation.

6 Sec. 3. Definition. – For the purpose of this Act and for the implementation of
7 the policy contained herein, the following definitions shall apply:

8 a. "Critical infrastructure" refers to extremely vital assets, systems, and
9 networks, whether physical or virtual, which destruction or disruption would
10 have a debilitating impact on national security, health and safety, or
11 economic well-being of citizens, or any combination thereof.

12 b. "Critical Information Infrastructure (CII)" refers to computer systems,
13 information and communications technology (ICT) networks, and digital
14 assets that are necessary for the continuous operation and delivery of the
15 critical infrastructure services of the country.

16 c. "CII institution" refers to a government agency or a private company that
17 owns, operates, controls, and/or maintains critical information
18 infrastructure, and whose operation is nationwide in scope and/or covers
19 metropolitan centers, including Metro Manila, Metro Cebu, Metro Davao,
20 and, by 2025, Metro Cagayan de Oro, or as defined and updated by the
21 National Economic Development Authority (NEDA) or the Philippine
22 Statistics Authority (PSA).

23 d. "Computer Emergency Response Team" or "CERT" refers to an organization
24 that studies computer and network security in order to:

- 25 i. provide incident response services to victims of attacks;
- 26 ii. publish alerts concerning vulnerabilities and threats, and;
- 27 iii. offer other information that aids in the improvement of computer and
28 network security.

29 e. "Information security" refers to the preservation of the confidentiality,
30 integrity, and availability of information. This may also involve other
31 properties, such as authenticity, accountability, non-repudiation, and
32 reliability of information.

- 1 f. "Information security incident" refers to an occurrence that actually or
2 potentially jeopardizes the confidentiality, integrity, or availability of an
3 information system or the information the system processes, stores, or
4 transmits or that constitutes a violation or imminent threat of violation of
5 security policies, security procedures, or acceptable use policies.
- 6 g. "Information system" refers to applications, services, information
7 technology assets, or any component handling information.
- 8 h. "International Electrotechnical Commission" or "IEC" refers to international
9 standards that are essential for quality and risk management, which help
10 researchers understand the value of innovation and allow manufacturers to
11 produce products of consistent quality and performance.
- 12 i. "International Organization for Standardization" or "ISO" refers to an
13 independent, non-governmental organization that develops and publishes
14 international standards to ensure the quality, safety and efficiency of
15 products, services and systems.

16 Sec. 4. Coverage of Critical Information Infrastructure. – This Act covers CII,
17 whether in the public or private sector, in industries including, but not limited to:

- 18 a. Government and Emergency Services;
19 b. Business Process Outsourcing;
20 c. Healthcare;
21 d. Media;
22 e. Banking
23 f. Financial;
24 g. Energy;
25 h. Water;
26 i. Telecommunications;
27 j. Transport and logistics.

28
29 An entity, whether public or private, that owns, operates, and maintains CII in
30 the industries mentioned above, and as updated by the Department of Information
31 and Communications Technology (DICT), shall be covered by this Act.

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

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

9 a. adopt the Code of Practice stipulated in the following:

- 10 i. Philippine National Standard (PNS) on *ISO/IEC 27001 Information*
11 *Security Management System (ISMS) series of standards;*
12 ii. PNS *ISO 22301 Security and Resilience – Business Continuity*
13 *Management Systems (BCMS); and*
14 iii. *ISO/IEC 27701 Privacy Information Management Systems, as*
15 applicable; or
16 iv. the latest standards adopted as PNS.

17 b. submit to the DICT a copy of their formal certification as proof of adoption
18 of the PNS ISO/IEC 27000 series of standards, PNS ISO 22301, and ISO/IEC
19 27701, as applicable; and

20 c. ensure that their certificates are up-to-date and shall submit the latest
21 annual audit confirmation to the DICT.

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

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

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

7 Sec. 6. National Computer Emergency Response Team (NCERT) as the
8 Centralized Information Security Incident Reporting Mechanism. – All covered CII
9 Institutions shall:

10 a. Report all information security incidents affecting their institutions to the
11 NCERT of the DICT, which shall be the central authority for all Sectoral and
12 Organizational CERTs in the country;

13 b. Submit an information security incident *detection* report to the NCERT
14 within twenty-four (24) hours upon detection of the incident(s). The report
15 shall contain basic information about the incident, such as:

16 i. date when the incident was first detected;

17 ii. nature of the information security incident;

18 iii. possible business processes and functions compromised; and

19 iv. agency's initial response and next steps.

20 c. Submit an incident *progress* report, upon request of the NCERT, in order to
21 help assess and provide the necessary support in responding to an incident;

22 d. Submit a *post-incident* report, which contains the following information: (i)
23 magnitude of business operations compromised, (ii) risk assessment, and
24 (iii) the agency's response. They shall also provide the necessary additional
25 information about the incident, as requested by the NCERT;

26 e. Compile on an annual basis a summary of all information security incident
27 reports and submit an annual report to the DICT Cybersecurity Bureau every
28 30th of June;

29 f. Comply with the reporting mechanism and template prescribed by the DICT,
30 in the submission of all the reporting requirements described above:
31 *Provided*, That information-sharing shall be done using established

1 communication protocol, using at the minimum, the Traffic Light Protocol
2 (TLP) as established by the DICT MC 2017-005 or succeeding policies;

- 3 g. Participate in activities that help promote awareness, capacity-building, and
4 improve an organization's information security readiness, protection, and
5 incident response capabilities, such as but not limited to, cyber drills.

6 **Sec. 7. Designation of Personnel with Information Security Credentials. – All**
7 **government agencies shall have at least one personnel with sufficient information**
8 **security training and credentials. Such personnel shall, preferably, hold at least**
9 **Division Chief *plantilla* position or any other position of equivalent rank, and perform**
10 **decision making or management functions. The DICT shall identify and release a list**
11 **of credentials that meet this requirement. Such personnel shall be the point person**
12 **for (i) compliance with prescribed standards, (ii) building information security**
13 **capability within the agency, and (iii) compliance with the reporting requirements of**
14 **the agency and NCERT.**

15 **Section 8. Compliance by all covered CII Institutions. –**

- 16 a. **Government compliance – The Department of Budget and Management**
17 **(DBM) shall review the submission by a CII Institution to the DICT of a**
18 **formal certification or self-declaration of compliance with any of the**
19 **prescribed information security standards, whichever submission applies, as**
20 **a prerequisite to budgetary approval. A government institution or sector**
21 **regulator, which itself operates or has jurisdiction over CII, shall comply**
22 **with the requirements set forth in this Act.**

- 23 b. **Non-government or private company compliance – Compliance with this Act,**
24 **specifically of Sections 5 and 6, shall be a prerequisite for the granting of**
25 **any regulatory approval, permit, and/or license to a private company**
26 **covered under Section 4 of this Act.**

27 **Sec. 9. Implementing Agency. – The DICT, through its Cybersecurity Bureau,**
28 **shall be the implementing agency of this Act, in accordance with the National**
29 **Cybersecurity Plan and relevant DICT policies. The DICT shall:**

- 30 a. **Create and maintain a database of all certifications, self-declaration, and**
31 **attestations of all covered CII institutions;**

- 1 b. Prescribe minimum information security standards for compliance by all CII
2 institutions;
- 3 c. Serve as the custodian for information security standards and incident
4 reports;
- 5 d. Collect and analyze all pertinent information about an information security
6 incident, and provide to government institutions, sectoral CERTs, and to the
7 public, a technical report of information security incidents for purposes of
8 policy, regulation, and providing guidance to all stakeholders on local
9 information security issues;
- 10 e. Prescribe a mechanism and template for the reporting of information
11 security incidents to the NCERT; and
- 12 f. Institute a consultation process and hold consultations to update the
13 coverage and definition of CII, minimum information security standards, and
14 recognize individual information security certifications every three (3) years
15 from the effectivity of this Act.

16 **Sec. 10. Responsibilities of the Department Heads and Sector Regulators with**
17 **jurisdiction over CII Institutions. – The heads of departments and sector regulators**
18 **who have a mandate over covered CII Institutions, including Sectoral CERT Leads as**
19 **identified in DICT Department Circular 003-2020, in coordination with the DICT, shall**
20 **be responsible for issuing the necessary policy and regulation that promote**
21 **information security and require compliance of CII institutions to the prevailing**
22 **standards to ensure information security and business continuity.**

23 **Sec. 11. Administrative Liability. – The respective heads of departments,**
24 **agencies, bureaus, offices, government-owned and controlled corporations (GOCCs)**
25 **and government financial institutions (GFIs), and State Colleges and Universities**
26 **(SUCs) shall be administratively liable for non-compliance with this Act pursuant to**
27 **existing laws, rules, and regulations.**

28 **Sec. 12. Funding. – The initial funding requirements for the implementation of**
29 **this Act shall be charged against the existing budget of the covered CII institutions**
30 **and such other appropriate funding sources as the DBM may identify, subject to**
31 **relevant laws, rules, and regulations.**

1 Sec. 13. Penalty. – Non-compliance with the provisions of this Act, whether or
2 not it results in data loss, breaches, hacking, or similar incidents, may result in
3 administrative, civil, or criminal liability under applicable laws, including but not limited
4 to, Republic Act No. 10175, also known as the "*Cybercrime Prevention Act of 2012*",
5 and Republic Act No. 10173, or the "*Data Privacy Act of 2012*".

6 Sec. 14. Annual Report. – Every 30th of April of every year, the DICT shall report
7 to the Office of the President the status of the implementation of this Act.

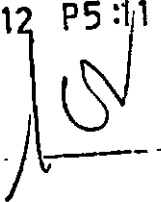
8 Sec. 15. Separability Clause. – If any provision of this Act is declared invalid or
9 unconstitutional, the remaining provisions not affected thereby shall continue to be in
10 full force and effect.

11 Sec. 16. Repealing Clause. – All laws, rules, and regulations inconsistent with
12 this Act are hereby repealed or modified accordingly.

13 Sec. 17. Effectivity. – This Act shall take effect fifteen (15) days following the
14 completion of its publication either in the Official Gazette or in two (2) newspapers of
15 general circulation in the Philippines.

Approved,

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

23 APR 12 P5 :11
RECEIVED BY 

SENATE

S.B. No. 2066

Introduced by SEN. WIN GATCHALIAN

AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS
TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS
AND INFRASTRUCTURE

EXPLANATORY NOTE

More and more Filipino individuals and businesses rely on and increase their use of digital technologies, including the internet, to perform their daily tasks, especially during the COVID-19 pandemic. The pandemic has no doubt rapidly accelerated the country's digital transformation and digital economy.

On average, Filipinos are estimated to use and consume 4.3 more digital services compared to pre-pandemic years and 95% of these pandemic consumers remain to be consumers today. Digital merchants are also getting tech-savvy as digital platforms, digital financial services and digital tools helped them survived the pandemic.¹ E-commerce also grew significantly, and sales are expected to be valued at US\$10.3 billion

¹ Google, Temasek, & Bain & Company (2021). *e-Conomy SEA 2021: Roaring 20s: The SEA digital divide*. https://services.google.com/fh/files/misc/philippines_e_conomy_sea_2021_report.pdf

by 2025.² Further, 53% of adult Filipinos were reported by the Bangko Sentral ng Pilipinas to have electronic money accounts in 2021, higher than 29% in 2019.³ Online education and remote work are also here to stay.⁴

With the increased use of digital technologies in our daily lives, malicious actors—from casual scammers to highly sophisticated state-backed groups—hunt for vulnerabilities in ICT systems and networks to steal information, disrupt essential services, and profit from attacks. Hence, it is critically important to ensure that the Philippines has a national policy framework for the protection of digital assets, especially critical information infrastructure (CII), against threats that could paralyze our economy and affect the wellbeing of Filipinos.

It is high time that we take the necessary steps to protect our CIIs by ensuring, at the minimum, compliance with international standards and globally accepted best practices for cybersecurity.

Thus, this measure seeks to protect the cybersecurity of CII by requiring the: (i) adoption of minimum information security standards, (ii) creation of a computer emergency response team and reporting of cybersecurity incidents, and (iii) development of a capable pool of cybersecurity professionals and practitioners that will be critical to the effective implementation of cybersecurity policy, rules, and standards. Simply put, this measure will provide a framework for ensuring the security and reliability of the

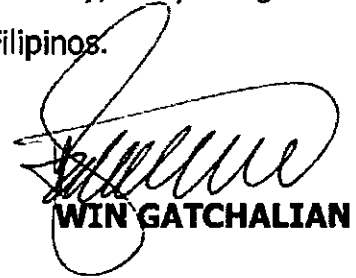
² GlobalData (9 Dec 2021). *Online shopping and rising internet penetration to lead Philippines e-commerce at 17% CAGR through 2025, forecasts GlobalData*. <https://www.globaldata.com/online-shopping-rising-internet-penetration-lead-philippines-e-commerce-17-cagr-2025-forecasts-globaldata/>

³ Villanueva, J. (24 Jan 2022). *PH digital transactions to grow despite challenges: BSP chief*. <https://www.pna.gov.ph/articles/1166236>; GCash alone grew 200% between 2020 and May 2022, now boasting 60 million users. See Cueto, F.E. (25 May 2022). *Gcash claims 60 million users in PH*. <https://www.manilatimes.net/2022/05/25/business/top-business/gcash-claims-60-million-users-in-ph/1844877>

⁴ World Bank (2020). *Building a resilient recovery. Philippines Economic Update: December 2020 edition*. <https://openknowledge.worldbank.org/bitstream/handle/10986/34899/Philippines-Economic-Update-Building-a-Resilient-Recovery.pdf>

country's digital ecosystem, which is crucial to the country's continued digitalization and growing digital economy.

As a necessary step to improving Philippine cybersecurity, the passage of this bill is earnestly sought for the security and well-being of all Filipinos.



WIN GATCHALIAN

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

23 APR 12 P5:11

RECEIVED BY: _____

[Handwritten Signature]

SENATE

S.B. No. 2066

Introduced by SEN. WIN GATCHALIAN

AN ACT

REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE

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

1 SECTION 1. *Title.* – This Act shall be known as the “*Critical Information*
2 *Infrastructure Protection Act of 2022.*”

3

4 SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of information
5 and communications technology in nation building. With the growth of information
6 computer technology (ICT), new and serious threats arising from its use and our reliance
7 on it in our daily lives surface and, as such, the State recognizes as vitally important the
8 establishment of a more secure cyberspace and a data protection regime that is compliant
9 with international standards and ensures the free flow of information.

10 It is hereby declared the policy of the State to protect Critical Information
11 Infrastructure (“CII”) from cyberattacks and threats, data manipulation, cybercrimes, and

1 activities of malicious actors. The State recognizes that the protection of computers,
2 networks, electronic devices, and digital assets, including information, is a common
3 objective and requires the combined efforts of the public and private sectors, and
4 cooperation with local and international actors, in order to minimize the impact of, if not
5 prevent, cyberattacks, threats, and risks on the nation's security and socio-economic well-
6 being.

7 Further, the adoption and implementation of minimum information security
8 standards is a globally accepted best practice to provide guidance, which would lead to
9 more efficient use of resources, improved risk management, consistent delivery of critical
10 and essential services, and effective protection of the confidentiality, integrity, and
11 availability of information that is vital to the nation.

12
13 SEC. 3. *Definition.* – For the purpose of this Act and for the implementation of the
14 policy contained herein, the following definitions shall apply:

- 15 a. "*Critical Infrastructure*" refers to assets, systems, and networks, whether
16 physical or virtual, that are considered so vital that their destruction or
17 disruption would have a debilitating impact on national security, health and
18 safety, or economic well-being of citizens, or any combination thereof.
- 19 b. "*Critical Information Infrastructure (CII)*" refers to computer systems, ICT
20 information and communications technology (ICT) networks, and digital assets
21 that are necessary for the continuous operation and delivery of the country's
22 critical infrastructure services.
- 23 c. "*CII Institution*" refers to a government agency or a private company that owns,
24 operates, controls, and/or maintains critical information infrastructure, and
25 whose operation is nationwide in scope and/or covers metropolitan centers,
26 including Metro Manila, Metro Cebu, Metro Davao, and, by 2025, Metro
27 Cagayan de Oro, or as defined and updated by the National Economic
28 Development Authority (NEDA) or the Philippine Statistics Authority (PSA).

- 1 d. "*Computer Emergency Response Team*" or "*CERT*" refers to an organization
2 that studies computer and network security in order to provide incident
3 response services to victims of attacks, publish alerts concerning vulnerabilities
4 and threats, and to offer other information to help improve computer and
5 network security.
- 6 e. "*Information security*" refers to the preservation of the confidentiality, integrity,
7 and availability of information. This may also involve other properties, such as
8 authenticity, accountability, non-repudiation, and reliability of information.
- 9 f. "*Information security incident*" refers to an occurrence that actually or
10 potentially jeopardizes the confidentiality, integrity, or availability of an
11 information system or the information the system processes, stores, or
12 transmits or that constitutes a violation or imminent threat of violation of
13 security policies, security procedures, or acceptable use policies.
- 14 g. "*Information system*" refers to applications, services, information technology
15 assets, or any component handling information.
- 16

17 SEC. 4. *Coverage of Critical Information Infrastructure.* – This Act covers CII,
18 whether in the public or private sector, in industries including, but not limited to:

- 19 a. Banking and finance;
20 b. Broadcast media;
21 c. Emergency services and disaster response;
22 d. Energy;
23 e. Health;
24 f. Telecommunications;
25 g. Transportation (land, sea, air); and
26 h. Water.

27 An entity, whether public or private, that owns, operates, and maintains CII in the
28 industries mentioned above, and as updated by the Department of Information and
29 Communications Technology (DICT), shall be covered by this Act.

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

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

9 They are required to:

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

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

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

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

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

10
11 **SEC. 6. *National Computer Emergency Response Team ("NCERT") as the***
12 ***Centralized Information Security Incident Reporting Mechanism.*** – All covered CII
13 Institutions shall:

- 14 a. Report all information security incidents affecting their institutions to the DICT's
15 Philippine National Computer Emergency Response Team, which shall be the
16 central authority for all Sectoral and Organizational CERTs in the country;
- 17 b. Submit an information security incident detection report to the NCERT within
18 twenty-four (24) hours upon detection of the incident(s). The report shall
19 contain basic information about the incident, such as: (1) date when the
20 incident was first detected, (ii) nature of the information security incident, (iii)
21 possible business processes and functions compromised, and (iv) agency's
22 initial response and next steps;
- 23 c. Submit an incident *progress* report, upon request of the NCERT, in order to
24 help assess and provide the necessary support in responding to an incident;
- 25 d. Submit a *post-incident* report, which contains the following information: (i)
26 magnitude of business operations compromised, (ii) risk assessment, and (iii)
27 the agency's response. They shall also provide the necessary additional
28 information about the incident, as requested by the NCERT;

- 1 e. Compile on an annual basis a summary of all information security incident
2 reports and submit an annual report to the DICT Cybersecurity Bureau every
3 30th of June;
- 4 f. Comply with the reporting mechanism and template prescribed by the DICT, in
5 the submission of all the reporting requirements described above: *Provided*,
6 that information-sharing shall be done using established communication
7 protocol, using at the minimum, the Traffic Light Protocol (TLP) as established
8 by the DICT MC 2017-005 or succeeding policies.
- 9 g. Participate in activities that help promote awareness, capacity building, and
10 improve an organization's information security readiness, protection, and
11 incident response capabilities, such as but not limited to cyber drills.
- 12

13 **SEC. 7. *Designation of Personnel with Information Security Credentials.*** – All
14 government agencies shall have at least one personnel with sufficient information security
15 training and credentials. Such personnel shall, preferably, hold at least Division Chief
16 plantilla position (or equivalent) and perform decision making or management functions.
17 The DICT shall identify and release a list of credentials that meet this requirement. Such
18 personnel shall be the point person for (i) compliance with prescribed standards, (ii)
19 building information security capability within the agency, and (iii) compliance with the
20 agency's and NCERT's reporting requirements.

21

22 **SEC. 8. *Compliance by all covered CII Institutions.***

23 a. ***Government compliance.*** - The Department of Budget and Management (DBM)
24 shall review the submission by a CII Institution to the DICT of a formal certification or
25 self-declaration of compliance with any of the prescribed information security standards,
26 whichever submission applies, as a prerequisite to budgetary approval. A government
27 institution or sector regulator, which itself operates or has jurisdiction over CII, shall
28 comply with the requirements set forth in this Act.

29 b. ***Non-government or private company compliance.*** - Compliance with this Act,
30 specifically of Sections 5 (standards) and 6 (reporting), shall be a prerequisite for the

1 granting of any regulatory approval, permit, and/or license to a private company covered
2 under Section 4 of this Act.

3
4 **SEC. 9. *Implementing Agency.*** – The DICT, through its Cybersecurity Bureau, shall
5 be the implementing agency of this Act, in accordance with the National Cybersecurity
6 Plan and relevant DICT policies. The DICT shall:

- 7 a. create and maintain a database of all certifications, self-declaration, and
8 attestations of all covered CII institutions;
- 9 b. prescribe minimum information security standards for compliance by all CII
10 institutions;
- 11 c. serve as the custodian for information security standards and incident reports;
- 12 d. collect and analyze all pertinent information about an information security
13 incident, and provide to government institutions, sectoral CERTs, and to the
14 public a technical report of information security incidents for purposes of policy,
15 regulation, and providing guidance to all stakeholders on local information
16 security issues;
- 17 e. prescribe a mechanism and template for the reporting of information security
18 incidents to the NCERT; and
- 19 f. institute a consultation process and hold consultations to update the coverage
20 and definition of CII, minimum information security standards, and recognize
21 individual information security certifications every three (3) years from the
22 effectivity of this Act.

23
24 **SEC. 10. – *Responsibilities of the Department Heads and Sector Regulators with***
25 ***jurisdiction over CII Institutions.*** - The heads of departments and sector regulators who
26 have a mandate over covered CII Institutions, including Sectoral CERT Leads as identified
27 in DICT DC 003-2020, in coordination with the DICT, shall be responsible for issuing the
28 necessary policy and regulation that promote information security and require compliance
29 of CII institutions to the prevailing standards to ensure information security and business
30 continuity.

1 SEC. 11. *Administrative Liability.* – The respective heads of departments, agencies,
2 bureaus, offices, GOCCs, GFIs, and SUCs shall be administratively liable for non-
3 compliance with this Act pursuant to existing laws, rules, and regulations.
4

5 SEC. 12. *Funding.* – The initial funding requirements for the implementation of this
6 Act shall be charged against the existing budget of the covered CII institutions and such
7 other appropriate funding sources as the DBM may identify, subject to relevant laws,
8 rules, and regulations.
9

10 SEC. 13. *Penalty.* – Non-compliance with the provisions of this Act, whether or not
11 it results in data loss, breaches, hacking, or similar incidents, may result in administrative,
12 civil, or criminal liability under applicable laws, including but not limited to Republic Act
13 No. 10175 also known as the Cybercrime Prevention Act of 2012 and Republic Act No.
14 10173 or the Data Privacy Act of 2012.
15

16 SEC. 14. *Annual Report.* – Every 30th of April of every year, the DICT shall report
17 to the Office of the President the status of the implementation of this Act.
18

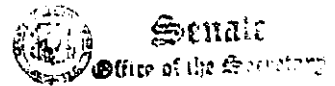
19 Sec. 15. *Separability Clause.* – If any provision of this Act is declared invalid or
20 unconstitutional, the remaining provisions not affected thereby shall continue to be in full
21 force and effect.
22

23 SEC. 16. *Repealing Clause.* – All laws, rules, and regulations inconsistent with this
24 Act are hereby repealed or modified accordingly.
25

26 SEC. 17. *Effectivity.* – This Act shall take effect fifteen (15) days following the
27 completion of its publication in two (2) newspapers of general circulation.

Approved,

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



23 JUL 17 P2:42

SENATE
S. No. 2316

RECEIVED BY:

Introduced by Senator MARK A. VILLAR

AN ACT
INSTITUTING A COMPREHENSIVE EARTHQUAKE MONITORING AND EARLY WARNING SYSTEM, APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The Philippines is located within the Pacific Ring of Fire, a region characterized by intense volcanic and seismic activities. The country has experienced a number of devastating earthquakes, which have resulted in loss of lives, damage to infrastructure and property, and economic disruption. In addition, it is feared that the "Big One" is already due to happen.

The key objective of this measure is to establish a nationwide, real-time earthquake monitoring system that detects, analyzes and provides early warning signals for seismic events. The system will gather robust data on seismic activity, enabling the government and disaster management agencies to respond more effectively to the risks posed by earthquakes.

The Philippine Institute of Volcanology and Seismology (PHIVOLCS) shall develop and implement a National Earthquake Monitoring and Early Warning System (NEMEWS) using the latest technology and best practices.

Advanced Earthquake Monitoring Centers shall be established within the PHIVOLCS regional offices, which shall collect and analyze data from seismic networks and provide accurate and timely earthquake monitoring services.

The PHIVOLCS shall establish a comprehensive network of seismic sensors strategically located throughout the country, with real-time data communication

equipment to facilitate rapid assessment and dissemination of earthquake information. An Earthquake Early Warning and Notification System shall be developed, allowing for the rapid distribution of warnings and alerts to the public and local government units.

This proposed measure represents a timely and critical investment in the country's disaster risk reduction and preparedness efforts. Instituting a comprehensive earthquake monitoring and early warning system will not only protect the lives and properties of millions of Filipinos but also minimize the economic and social impacts of these natural disasters.

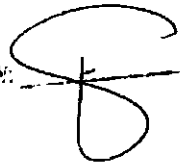
In view of the foregoing, the approval of this bill is sought.



MARK A. VILLAR

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

23 JUL 17 P2:42

RECEIVED BY: 

SENATE
S. No. 2316

Introduced by Senator MARK A. VILLAR

**AN ACT
INSTITUTING A COMPREHENSIVE EARTHQUAKE MONITORING AND EARLY
WARNING SYSTEM, APPROPRIATING FUNDS THEREFOR, 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 "Philippine Advanced
2 Earthquake Monitoring and Early Warning System Act of 2023."

3 Sec. 2. *Declaration of Policy.* – The State recognizes the need for a reliable and
4 advanced earthquake monitoring and early warning system to enhance public safety,
5 reduce damage to property, and minimize the loss of lives during any earthquake event.

6 The State shall, therefore, invest in developing, implementing, and maintaining a
7 comprehensive earthquake monitoring and early warning system and shall promote
8 community preparedness, information dissemination, and coordination among relevant
9 government agencies and local government units (LGUs).

10 Sec. 3. *National Earthquake Monitoring and Early Warning System.* – The Philippine
11 Institute of Volcanology and Seismology (PHIVOLCS) shall develop and implement a
12 National Earthquake Monitoring and Early Warning System (NEMEWS) using the latest
13 technology and best practices.

1 The NEMEWS shall have the following components;

2 (a) Advanced earthquake monitoring centers;

3 (b) A network of seismic sensors and real-time data communication equipment;

4 (c) An earthquake early warning and notification system;

5 (d) A public information dissemination and communication campaign; and

6 (e) Research and development programs for system improvements.

7 *Sec. 4. Establishment of Advanced Earthquake Monitoring Centers.* – Advanced
8 Earthquake Monitoring Centers shall be established within the PHIVOLCS regional offices.
9 These centers shall collect and analyze data from seismic networks and provide accurate
10 and timely earthquake monitoring services.

11 *Sec. 5. Network of Seismic Sensors and Real-Time Data Communication.* – The
12 PHIVOLCS shall establish a comprehensive network of seismic sensors strategically
13 located throughout the country, with real-time data communication equipment to
14 facilitate rapid assessment and dissemination of earthquake information.

15 *Sec. 6. Earthquake Early Warning and Notification System.* – An Earthquake Early
16 Warning and Notification System shall be developed, allowing for the rapid distribution of
17 warnings and alerts to the public and LGUs.

18 *Sec. 7. Public Information Dissemination and Communication Campaign.* – The
19 PHIVOLCS, in coordination with relevant government agencies, shall implement
20 information dissemination campaigns, community preparedness workshops, and regular
21 briefings for LGUs on earthquake hazards, preparedness, and response.

22 *Sec. 8. Research and Development.* – The PHIVOLCS shall continuously conduct
23 research and development intended to enhance the system's performance, introduce
24 innovative solutions, and ensure compatibility with international standards and best
25 practices.

26 *Sec. 9. Funding.* - The amount necessary for the effective implementation of this
27 Act shall be sourced from the current fiscal year's appropriation of PHIVOLCS under the
28 General Appropriations Act (GAA). Additional funding may be sourced from existing
29 appropriations for similar purposes, international loans, grants, or any other funding
30 sources.

1 Sec. 10. *Implementing Rules and Regulations.* - The Department of Science and
2 Technology (DOST) and PHIVOLCS, in consultation with the Department of Information
3 and Communications Technology (DICT) and other relevant government agencies and
4 stakeholders, shall promulgate the implementing rules and regulations necessary to carry
5 out the provisions of this Act within ninety (90) days from its effectivity.

6 Sec. 11. *Separability Clause.* – Any portion or provisions of this Act that may be
7 declared unconstitutional or invalid and shall not have the effect of nullifying other
8 portions or provisions hereof as long as such remaining portions or provisions can still
9 subsist and be given effect in their entirety.

10 Sec. 12. *Repealing Clause.* – All laws, presidential decrees, executive orders,
11 memoranda, circulars, and other issuances, or parts thereof, which are inconsistent with
12 the Act, are hereby repealed or modified accordingly.

13 Sec. 13. *Effectivity Clause.* – This Act shall be take effect fifteen (15) days after its
14 publication in at least two (2) newspapers of general circulation.

Approved,