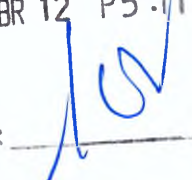


NINETEENTH CONGRESS OF THE]
REPUBLIC OF THE PHILIPPINES]
First Regular Session]

23 ABR 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_economy_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

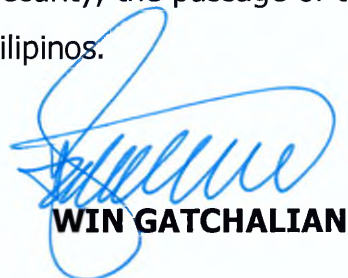
² GlobalData (9 Dec 2021). *Online shopping and rising internet penetration to lead Philippines e-commerce at 17% CAGR through 2025, forecasts GlobalData*. <https://www.globaldata.com/online-shopping-rising-internet-penetration-lead-philippines-e-commerce-17-cagr-2025-forecasts-globaldata/>

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: 

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,