Senate
Office of the Secretary

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

23 JAN 18 P5 :24

RECEIVED BY:

SENATE
S. No. 1701

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 [1]and third most extorted by ransomware[2]. Continued vulnerability to data breaches could cost an average of PHP 250 million[3], 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

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

SENATE

S. No. 1701

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:

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

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

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

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

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

a. "Critical infrastructure" refers to assets, systems, and networks, whether physical or virtual, that are considered so vital that their destruction or disruption would have a debilitating impact on national security, health and safety, or economic well-being of citizens, or any combination thereof.

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

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

d. "Computer Emergency Response Team" or "CERT" refers to an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.

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.

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

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

They are required to:

a. adopt the Code of Practice stipulated in the Philippine National Standard (PNS) on *ISO/IEC 27001 Information Security Management System (ISMS) (series of standards)* and PNS *ISO 22301 Security and resilience – Business continuity management systems (BCMS)*. They shall also adopt the *ISO/IEC 27701 Privacy Information Management Systems,* as applicable;

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

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

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

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

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

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

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

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

a. report all information security incidents affecting their institutions to the DICT's Philippine National Computer Emergency Response Team, which shall be the central authority for all Sectoral and Organizational CERTs in the country;

b. submit an information security incident *detection* report to the NCERT within twenty-four (24) hours upon detection of the incident(s). The report shall contain basic information about the incident, such as: (1) date when the incident was first detected, (ii) nature of the information security incident, (iii) possible business processes and functions compromised, and (iv) agency's initial response and next steps;

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

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

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

f. comply with the reporting mechanism and template prescribed by the DICT, in the submission of all the reporting requirements described above: *Provided*, that information-sharing shall be done using established communication protocol, using at the minimum, the Traffic Light Protocol (TLP) as established by the DICT MC 2017-005 or succeeding policies.

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

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

Sec. 8. Compliance by all covered CII Institutions.

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

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

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

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

b. prescribe minimum information security standards for compliance by all CII institutions;

c. serve as the custodian for information security standards and incident reports;

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

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

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

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

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

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

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

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

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

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

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

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

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

Approved.