Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

NINETEENTH CONGRESS

First Regular Session

HOUSE BILL NO. 5940

INTRODUCED BY REPRESENTATIVE JURDIN JESUS M. ROMUALDO

EXPLANATORY NOTE

This bill seeks to strengthen the capability and define further the functions of the Department of Information and Communications Technology (DICT) in handling "Critical Information Infrastructure" (CII) and set minimum information security standards.

There are various critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are vital to the country and their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The DICT can collaborate and coordinate with different sector stakeholders to ensure that valuable information can be shared, protected and accessed in a secure environment. Government must be proactive and innovative as imminent threats are lurking around and becoming immensely destructive upsetting and incapacitating services with potential losses estimated to reach Billions of pesos daily from illegal perpetrators according to industry experts.

Government must provide ways to manage risk and upgrade current resilience standards in close partnership with stakeholders within the critical infrastructure sectors. By engaging stakeholders participation, DICT and relevant government agencies such as the National Security Council and the National Economic and Development Authority can address gaps and provide technical assistance to these CII sectors and institutionalizing a National Computer Emergency Response Team (NCERT) for sectoral and organizational computer emergency response teams.

Cybersecurity incidents such as threats and attacks should be reported to the NCERT for appropriate action and to alert these sectors from these cybersecurity breaches and attacks.

Presently, we have different laws in place such as: R.A. No. 11659 (Public Service Act Amendment of 2022), R.A. 11479 (Anti-Terrorism Act of 2020), Republic Act No. 10175 ("Cybercrime Prevention Act of 2012), National Cyber Security Plans, DICT MC No. 005 (August 2017), Office of the President MO No. 37, Series of 2001 but we need to regularly update and upgrade these policies to meet present and future threats to CII Sectors.

DICT must provide the policy protocols and determine if these CIIs for both government and private sectors to determine their compliance with these minimum standards, assess how they manage and implement their own security standards, and internal compliance evaluation.

We understand these challenges and that not all industries will be able to provide and comply with these minimum standards especially the micro and small enterprises. Thus, it is suggested that we classify the Critical Infrastructures according to its size and scope of operations, potential threats, economic impact and public exposures.

Our focus is to strengthen our capabilities to withstand these threats and protect critical information infrastructures from imminent and potential breaches and security threats. Most prone CII Sectors are from: Government, Banking and Finance, Broadcast Media, Business Process Outsourcing, Energy, Water, Health, Telecommunications and Transportation.

Industry sources have pinpointed in a webinar entitled "Philippine Cybersecurity: Issues and Priority Reforms" sponsored by Senate Economic Planning Office (SEPO) in partnership with the Offices of Senator Grace L. Poe and Senator Alan Peter S. Cayetano and Secure Connections last October 25, 2022, the notable cyberattacks in the past 5 years in these sectors:

1.) Health Sector:
SingHealth of Singapore (2018): hackers stole personal information of 1.5 million patients;
2.) Water Sector:
Israel (2020) water treatment systems hackers attempted to alter their chlorine levels;
3.) Financial Institution:
Philippine bank (June 2020) malware was used to transfer Php 170 million to various accounts and withdrawn immediately;
4.) Pipeline:
US Colonial Pipeline (2021) ransomware attack led to shutdown of pipeline carrying 45% of East Coast fuel supplies;
5.) Telecommunications
Australian Telco Optus successfully breached affecting 10 million clients or 40% of Australia's population.

Each day, our critical information infrastructure sectors are very prone to cyberattacks from spyware, malware, ransomware, phishing, Denial of Service, viruses, and such other illegal cyber activities. We urgently need to address this and invest on prevention and proper impact management with the right system protocols compliant with industry standards.

The support of the Members of Congress for the approval of this bill is highly enjoined.

JURDIN JESUS M. ROMUALDO

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

NINETEENTH CONGRESS

First Regular Session

HOUSE BILL NO. **5940**

INTRODUCED BY REPRESENTATIVE JURDIN JESUS M. ROMUALDO

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

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

SECTION 1. Short Title – This Act shall be known as the *"Critical Information Infrastructure Protection Act."*

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 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 cyber-attacks 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, cyber-attacks, 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 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, CT 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 any 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, 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. Business process outsourcing;
d. Emergency services and disaster response;
e. Energy;
f. Government;
g. Health;
h. Telecommunications;
i. Transportation (land, sea, air); and
j. 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.

Sec. 5. Classification Criteria Critical Information Infrastructure. – All covered CII institutions shall be classified according to a criterion set down by this Act:

a. Size – size or geographical scope of operation in key sectors;
b. Casualties effects – potential number of fatalities or injuries;
c. Economic effects – significance of economic loss and/or degradation of products and services, including potential environmental effects; and
d. Public effects – impact on public confidence, physical suffering, and disruption of daily life, including the loss of essential services.

Sec. 6. 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 shall be required to:

a. Adopt the Code of Practice stipulated in the Philippine National Standard (PNS) on Information Security Management System (ISMS) (series of standards) and PNS ISO Security and resilience - Business continuity management systems (BCMS). They shall also adopt the Privacy Information Management System as applicable;

b. Submit to the DICT a copy of their formal certification as proof of adoption of the previous stipulation as applicable;

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.

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. 7. 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 CERT's in the country;

b. Require all CII institutions to report cybersecurity incidents to NCERT within twenty-four (24) hours upon detection of the incident(s);

c. 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: (i) 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;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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. 8. 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. 9. 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 6 (standards) and 7 (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. 10. 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. update the definition of CII, list of CII institutions, and the sector or industry covered as CII every three (3) years;
c. prescribe and update minimum information security standards for compliance by all CII institutions;
d. determine and update information security standards, and require CII institutions to comply with such standards, as it deems it necessary and appropriate.
e. serve as the custodian for information security standards, incident reports, and credentials for personnel;

f. 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.

g. strengthen mandate to manage NCERT, and prescribe a mechanism and template for the reporting of information security incidents to the NCERT; and

h. 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.

In addition, the National Security Council (NSC) and National Economic and Development Authority (NEDA) shall be tasked to: (1) provide inputs to the DICT for the definition of CI, CI sectors, and CI institutions CII institutions; and (2) participate in the consultations conducted by the DICT or the updating the definition of CII, list of CII institutions, and CII sectors.

Sec. 11. – Government Agency or Sector Regulator. There shall be an appropriate sector agency which would have the following rol

a. As an administrative agency or regulator – issue policy and regulation requiring compliance of CII institutions under their jurisdiction with prevailing standards, as prescribed by the DICT or higher;

b. As a CII institution – adopt programs, guidelines, and written procedures for the implementation of its chosen information security standard, including submission of updated certification to the DICT; and

c. Participate in consultations conducted by the DICT for updating the definition of CII, list of CII institutions, and CII sectors.

Sec. 12. - 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, 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 based on standards prescribed by DICT (or higher).

Sec. 13. 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. 14. 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. 15. 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. 16. 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. 17. 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. 18. Repealing Clause. - All laws, rules, and regulations inconsistent with this Act are hereby repealed or modified accordingly.

Sec. 19. Effectivity. -This Act shall take effect fifteen (15) days following the completion of its publication in two (2) newspapers of general circulation.

Approved,