

Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

TWENTIETH CONGRESS

First Regular Session

House Bill No. 620



INTRODUCED BY REPRESENTATIVE JURDIN JESUS M. ROMUALDO

EXPLANATORY NOTE

“Cybersecurity is no longer optional—it is essential to national survival.”

This bill seeks to strengthen the institutional capacity of the Department of Information and Communications Technology (DICT) in protecting Critical Information Infrastructure (CII), define its functions, and establish minimum cybersecurity standards for both government and private sectors. It also mandates the establishment and institutionalization of a National Computer Emergency Response Team (NCERT).

Across the globe and here at home, cybersecurity threats are increasing in scale, complexity, and damage, often targeting vital sectors whose disruption can paralyze services and endanger national welfare. CII sectors—including government, banking and finance, broadcast media, business process outsourcing, energy, water, health, telecommunications, and transportation—are at particular risk. The incapacitation of any of these sectors would have a debilitating impact on public safety, national security, and economic stability.

The following are the recent events illustrating this urgent reality:

- In January 2025, a major denial-of-service (DDoS) attack disrupted the websites of key academic institutions under the edu.ph domain, including UP, UST, and PUP¹;
- In March 2025, the hacker “ph1ns” leaked data allegedly obtained from the National Telecommunications Commission (NTC)²;
- In February 2025, the Philippine Army confirmed that cybercriminals breached its networks and accessed sensitive personnel information³;
- In 2024, the Philippine Coast Guard’s X (Twitter) account was compromised, while a DICT Disaster Risk Reduction website was defaced⁴; and
- Ransomware and phishing cases reportedly doubled in 2023, with estimated losses of up to ₱55 million per incident, especially among financial institutions and SMEs⁵

¹Philippine Star, “DDoS attacks hit.edu.ph domains”, January 2025.

² Inquirer.net, “Hacker leaks data allegedly from NTC”, March 2025.

³ Reuters, “Philippine Army confirms cyber intrusion”, February 2025.

⁴ Philippine News Agency, “DICT’s DRRM site defaced; PCG X account hacked”, February–July 2024.

⁵ DICT, Cybersecurity Bureau Briefing; TrendMicro PH Report 2023.

Globally, CII-related cyberattacks have resulted in devastating consequences:

- **HEALTH SECTOR:** In 2018, hackers stole medical records of 1.5 million patients in the SingHealth breach in Singapore.
- **WATER SECTOR:** In 2020, threat actors attempted to manipulate chlorine levels in Israeli water facilities.
- **PIPELINE:** In 2021, a ransomware attack on the Colonial Pipeline in the U.S. disrupted nearly half of East Coast fuel supply.
- **TELECOMMUNICATIONS:** In 2022, the Optus data breach in Australia affected over 10 million users.
- **FINANCIAL INSTITUTION:** In 2020, malware enabled unauthorized transfers of ₱170 million from a Philippine bank.⁶

To address the growing threat landscape, this measure empowers the DICT to:

1. Define and regularly update minimum information security standards for CIIs;
2. Lead interagency and multi-sectoral coordination efforts to safeguard critical assets;
3. Institutionalize and operationalize a National Computer Emergency Response Team (NCERT) that shall oversee and respond to cyber threats in real time;
4. Classify CII sectors based on size, scope, risk exposure, and economic or public impact, with consideration for the compliance capacity of micro and small enterprises; and
5. Establish compliance reporting and audit protocols to assess adherence to national cybersecurity frameworks.

Although the country already has related laws and policies—such as Republic Act Nos. 11659 (Amended Public Service Act), 11479 (Anti-Terrorism Act of 2020), 10175 (Cybercrime Prevention Act of 2012), the National Cybersecurity Plan 2022, DICT Memorandum Circular No. 005, s. 2017, and Memorandum Order No. 37, s. 2001—these frameworks must be updated and harmonized to address evolving digital threats and strengthen cyber resilience.

Through proactive governance and stakeholder engagement, the government can help ensure that our CII sectors are not only secure but also resilient. It is in this context that the swift passage of this bill is earnestly sought.



JURDIN JESUS M. ROMUALDO

⁶ Senate Economic Planning Office, “Philippine Cybersecurity: Issues and Priority Reforms,” webinar proceedings, October 25, 2022.

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

TWENTIETH CONGRESS
First Regular Session
HOUSE BILL NO. 620

INTRODUCED BY REPRESENTATIVE JURDIN JESUS M. ROMUALDO

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

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

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

3
4 **SEC. 2. Declaration Policy** – The growth of information computer technology is
5 accompanied by new and serious threats and, as such, the state recognizes as vitally important the
6 establishment of a more secure cyberspace and data protection regime that is compliant with
7 international standards and ensures the free flow of information.

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

16
17 Further, the adoption and implementation of minimum information security standards is a
18 globally accepted best practice to provide guidance, which would lead to more efficient use of
19 resources, improved risk management, consistent delivery of critical and essential services, and
20 effective protection of the confidentiality, integrity, and availability of information that is vital to
21 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 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 a 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 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 regular 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 Institution 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;

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

4
5 **SEC. 8. Designation of Personnel with Information Security Credentials.** – All
6 government agencies shall have at least one personnel with sufficient information security training
7 and credentials. Such personnel shall, preferably, hold at least Division Chief Plantilla position (or
8 equivalent) and perform decision making or management functions. The DICT shall identify and
9 release a list of credentials that meet this requirement. Such personnel shall be the point person for
10 (i) compliance with prescribed standards, (ii) building information security capability within the
11 agency, and (iii) compliance with the agency's and NCERT's reporting requirements.

12
13 **SEC. 9. Compliance by all covered CII institutions.**

- 14
15 a. Government compliance: The Department of Budget and Management (DBM) shall
16 review the submission by a CII Institution to the DICT of a formal certification or self-
17 declaration of compliance with any of the prescribed information security standards,
18 whichever submission applies, as a prerequisite to budgetary approval. A government
19 institution or sector regulator, which itself operates or has jurisdiction over CII, shall
20 comply with the requirements set forth in this Act.
- 21 b. Non-government or private company compliance: Compliance with this Act,
22 specifically of Section 6 (standards) and Section 7 (reporting), shall be a prerequisite
23 for the granting of any regulatory approval, permit, and/or license to a private company
24 covered under Section 4 of this Act.

25
26 **SEC. 10. Implementing Agency.** – The DICT, through its Cybersecurity Bureau, shall be
27 the implementing agency of this Act, in accordance with the National Cybersecurity Plan and
28 relevant DICT policies. The DICT shall:

- 29
30 a. create and maintain a database of all certifications, self-declaration, and attestations of
31 all covered CII institutions;
- 32 b. update the definition of CII, list of CII institutions, and the sector or industry covered
33 as CII every three (3) years;
- 34 c. prescribe and update minimum information security standards for compliance by all
35 CII institutions;
- 36 d. determine and update information security standards, and require CII institutions to
37 comply with such standards, as it deems it necessary and appropriate;
- 38 e. serve as the custodian for information security standards, incident reports, and
39 credentials for personnel;
- 40 f. collect and analyze all pertinent information about an information security incident,
41 and provide to government institutions, sectoral CERTs, and to the public a technical
42 report of information security incidents for purposes of policy, regulation, and

1 providing guidance to all stakeholders on local information security issues.

- 2 g. strengthen mandate to manage NCERT, and prescribe a mechanism and template for
3 the reporting of information security incidents to the NCERT; and
4 h. institute a consultation process and hold consultations to update the coverage and
5 definition of CII, minimum information security standards, and recognize individual
6 information security certifications every three (3) years from the effectivity of this Act.

7
8 In addition, the National Security Council (NSC) and National Economic and Development
9 Authority (NEDA) shall be tasked to: (1) provide inputs to the DICT for the definition of CI, CI
10 sectors, and CI institutions CII institutions; and (2) participate in the consultations conducted by
11 the DICT or the updating the definition of CII, list of CII institutions, and CII sectors.

12
13 **SEC. 11. Government Agency or Sector Regulator.** There shall be an appropriate sector
14 agency which would have the following rol

- 15
16 a. As an administrative agency or regulator – issue policy and regulation requiring
17 compliance of CII institutions under their jurisdiction with prevailing standards, as
18 prescribed by the DICT or higher;
19 b. As a CII institution – adopt programs, guidelines, and written procedures for the
20 implementation of its chosen information security standard, including submission of
21 updated certification to the DICT; and
22 c. Participate in consultations conducted by the DICT for updating the definition of CII,
23 list of CII institutions, and CII sectors.

24
25 **SEC. 12. Responsibilities of the Department Heads and Sector Regulators with**
26 **jurisdiction over CII institutions.** The heads of departments and sector regulators who have a
27 mandate over covered CII institutions, including Sectoral CERT Leads as identified in DICT DC
28 003-2020, shall be responsible for issuing the necessary policy and regulation that promote
29 information security and require compliance of CII institutions to the prevailing standards to
30 ensure information security and business continuity based on standards prescribed by DICT (or
31 higher).

32
33 **SEC. 13. Administrative Liability.** – The respective heads of departments, agencies,
34 bureaus, offices, GOCCs, GFIs, and SUCs shall be administratively liable for non-compliance with
35 this Act pursuant to existing laws, rules and regulations.

36
37 **SEC. 14. Funding.** – The initial funding requirements for the implementation of this Act
38 shall be charged against the existing budget of the covered CII institutions and such other
39 appropriate funding sources as the DBM may identify, subject to relevant laws, rules, and
40 regulations.

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

6
7 **SEC. 16. Annual Report.** – Every 30th of April of every year, the DICT shall report to the
8 Office of the President the status of the implementation of this Act.

9
10 **SEC. 17. Separability Clause.** – If any provision of this Act is declared invalid or
11 unconstitutional, the remaining provisions not affected thereby shall continue to be in full force
12 and effect.

13
14 **SEC. 18. Repealing Clause.** – All laws, rules, and regulations inconsistent with this Act
15 are hereby repealed or modified accordingly.

16
17 **SEC. 19. Effectivity.** – This Act shall take effect fifteen (15) days following the
18 completion of its publication in two (2) newspapers of general circulation.

Approved,