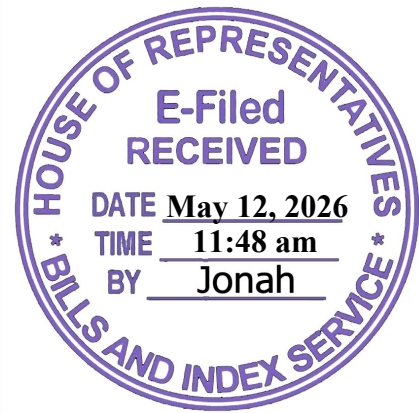


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session



HOUSE BILL NO. 9197

Introduced by **REPRESENTATIVE AUDREY KAY T. ZUBIRI**

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

EXPLANATORY NOTE

The rapid digital transformation of the Philippines has integrated information and communications technology (ICT) into the very fabric of our national life. While this growth fosters economic opportunity, it simultaneously exposes our Critical Information Infrastructure (CII)—the digital backbone of our energy, water, telecommunications, and financial sectors—to increasingly sophisticated cyber threats.

The proposed Critical Information Infrastructure Protection Act seeks to establish a robust, mandatory framework for securing the assets and networks that are so vital that their disruption would have a debilitating impact on national security and public safety.

Currently, the security posture of essential service providers varies significantly across industries. This bill addresses these gaps through the following:

- Requiring CII institutions to adopt globally recognized benchmarks;
- Allowing institutions the alternative of annual self-assessments using established frameworks like CIS Controls or NIST SP 800-53 to ensure that even smaller essential entities can maintain a high security baseline; and

- Establishing the National Computer Emergency Response Team (NCERT) as a central authority, mandating a strict 24-hour incident reporting rule to ensure rapid national coordination during a cyber crisis.

The bill recognizes that cybersecurity is a shared responsibility. It covers critical sectors including Banking and Finance, Energy and Water, Health and Emergency Services, and Telecommunications and Transportation.

By linking compliance to budgetary approvals for government agencies and regulatory permits for the private sector, this measure ensures that cybersecurity is no longer treated as an optional expense, but as a fundamental prerequisite for doing business in the Philippines. In view of the increasing frequency of global cyberattacks on critical infrastructure, the immediate passage of this bill is earnestly sought to protect the socio-economic well-being of every Filipino.



AUDREY KAY T. ZUBIRI
Representative, 3rd District of Bukidnon

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 9197

Introduced by **REPRESENTATIVE AUDREY KAY T. ZUBIRI**

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

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

1 **SECTION 1.** This Act shall be known as the “*Critical Information Infrastructure*
2 *Protection Act.*”
3

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

8 It is the policy of the State to protect Critical Information Infrastructure ("CII") from
9 cyberattacks and threats, data manipulation, cybercrimes, and activities of malicious actors.

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

15 Further, the adoption and implementation of minimum information security standards
16 is a globally accepted best practice to provide guidance, which would lead to more efficient
17 use of resources, improved risk management, consistent delivery of critical and essential

1 services, and effective protection of the confidentiality, integrity, and availability of
2 information that is vital to the nation.

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

- 6 a) "Critical infrastructure" refers to assets, systems, and networks, whether
7 physical or virtual, that are considered so vital that their destruction or
8 disruption would have a debilitating impact on national security, health and
9 safety, or economic well-being of citizens, or any combination thereof.
- 10 b) "Critical Information Infrastructure (CII)" refers to computer systems, ICT
11 information and communications technology (ICT) networks, and digital assets
12 that are necessary for the continuous operation and delivery of the country's
13 critical infrastructure services.
- 14 c) "CII institution" refers to a government agency or a private company that owns,
15 operates, controls, and/or maintains critical information infrastructure, and
16 whose operation is nationwide in scope and/or covers metropolitan centers,
17 including Metro Manila, Metro Cebu, Metro Davao, and, by 2025, Metro
18 Cagayan de Oro, or as defined and updated by the National Economic
19 Development Authority (NEDA) or the Philippine Statistics Authority (PSA).
- 20 d) "Computer Emergency Response Team" or "CERT" refers to an organization
21 that studies computer and network security in order to provide incident response
22 services to victims of attacks, publish alerts concerning vulnerabilities and
23 threats, and to offer other information to help improve computer and network
24 security.
- 25 e) "Information security" refers to the preservation of the confidentiality, integrity,
26 and availability of information. This may also involve other properties, such as
27 authenticity, accountability, non-repudiation, and reliability of information.
- 28 f) "Information security incident" refers to an occurrence that actually or
29 potentially jeopardizes the confidentiality, integrity, or availability of an
30 information system or the information the system processes, stores, or transmits
31 or that constitutes a violation or imminent threat of violation of security policies,
32 security procedures, or acceptable use policies.
- 33 g) "Information system" refers to applications, services, information technology
34 assets, or any component handling information.

1
2 **Sec. 4. Coverage of Critical Information Infrastructure.** — This Act covers CII,
3 whether in the public or private sector, in industries including, but not limited to:

- 4 a) Banking and finance;
5 b) Broadcast media;
6 c) Emergency services and disaster response;
7 d) Energy;
8 e) Health;
9 f) Telecommunications;
10 g) Transportation (land, sea, air); and
11 h) Water.

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

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

18
19 **Sec. 5. Adoption of Minimum Information Security Standards.** — All covered CII
20 institutions shall adopt and implement adequate measures to protect their ICT systems and
21 infrastructure, and respond to and recover from any information security incident, in
22 compliance with existing laws, rules and regulations, including the following:

- 23 a) adopt the Code of Practice stipulated in the Philippine National Standard (PNS) on
24 ISO/IEC 27001 Information Security Management System (ISMS) (series of standards)
25 and PNS ISO 22301 Security and resilience Business continuity management systems
26 (BCMS). They shall also adopt the ISO/IEC 27701 Privacy Information Management
27 Systems, as applicable;
28 b) submit to the DICT a copy of their formal certification as proof of adoption of the PNS
29 ISO/IEC 27000 (series of standards), PNS ISO 22301, and ISO/IEC 27701, as
30 applicable; and
31 c) ensure that their certificates are up-to-date and shall submit the latest annual audit
32 confirmation to the DICT.

33 In lieu of the submission of formal certification above, covered CII institutions shall
34 subject themselves to an annual information security self-assessment using standards, such as

1 but not limited to, the Center for Internet Security (CIS) Controls or the National Institute of
2 Standards and Technology (NIST) Special Publication (SP) 800-53, during the first quarter of
3 each year. The concerned institution shall submit this self-declaration and attest to its validity
4 to the DICT on or before the 31st of March. The self-declaration shall be signed off by the
5 respective head of the department directly in charge of the agency's information security
6 systems.

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

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

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

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

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

Section 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.

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

4 The DICT shall:

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

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

28
29 **Sec. 11. Appropriations.** — The initial funding requirements for the implementation of
30 this Act shall be charged against the existing appropriations of the covered CII institutions and
31 such other appropriate funding sources as the DBM may identify, subject to relevant laws,
32 rules, and regulations.

1 **Sec. 12. *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,
3 or criminal liability under applicable laws, including but not limited to Republic Act No. 10175
4 also known as the Cybercrime Prevention Act of 2012 and Republic Act No. 10173 or the Data
5 Privacy Act of 2012.
6

7 **Sec. 13. *Annual Report.*** — Every 30th of April of every year, the DICT shall report to
8 the Office of the President the status of the implementation of this Act.
9

10 **Sec. 14. *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. 15. *Repealing Clause.*** — All laws, rules, and regulations inconsistent with this
15 Act are hereby repealed or modified accordingly.
16

17 **Sec. 16. *Effectivity.*** — This Act shall take effect fifteen (15) days after its publication
18 in the Official Gazette or in a newspaper of general circulation.
19

20 *Approved,*