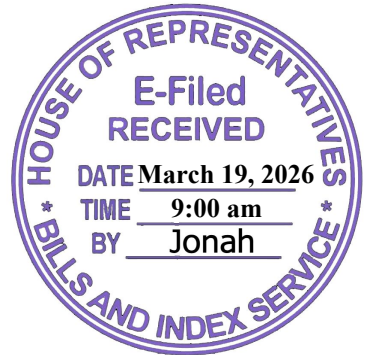




Republic of the Philippines  
HOUSE OF REPRESENTATIVES  
Quezon City, Metro Manila

Twentieth Congress  
First Regular Session

HOUSE BILL NO. 8707



---

Introduced by Representatives JOCELYN P. TULFO and RALPH WENDEL P. TULFO

---

**AN ACT ESTABLISHING THE PHILIPPINE CRITICAL INFORMATION  
INFRASTRUCTURE PROTECTION FRAMEWORK, MANDATING CYBERSECURITY  
STANDARDS FOR VITAL INDUSTRIES, PROVIDING CYBER-DEFENSE GRANTS  
FOR SMALL AND MEDIUM ENTERPRISES, AND APPROPRIATING FUNDS  
THEREOF**

**EXPLANATORY NOTE**

The digital transformation of the Philippine economy has brought unprecedented growth, but it has also exposed our most vital systems to severe, escalating risks. Recent reports from the Armed Forces of the Philippines and various intelligence sectors have highlighted persistent, highly sophisticated cyber espionage and sabotage campaigns targeting our national networks. These state-sponsored and transnational threats do not just compromise data; they threaten our power grids, financial systems, agricultural supply chains, and national security.

While the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) penalizes individual cyber offenses, the Philippines currently lacks a comprehensive, proactive legislative framework specifically designed to harden Critical Information Infrastructure (CII) and defend against systemic, nation-state-level cyberattacks. Furthermore, our Small and Medium Enterprises (SMEs), which form the backbone of our export and domestic supply chains, often lack the capital to defend themselves against these advanced persistent threats (APTs).

This bill, the **"Philippine Critical Information Infrastructure and Cybersecurity Resilience Act,"** shifts our national posture from reactive to fortified. It mandates strict cybersecurity standards for critical industries, establishes a mandatory incident reporting framework to the Department of Information and Communications Technology (DICT), creates a financial grant program to subsidize cybersecurity for vulnerable SMEs, and formally integrates cyber defense protocols into our national disaster and emergency response systems.

To secure our digital borders and ensure the uninterrupted operation of the Philippine economy, the immediate passage of this bill is earnestly sought.

  
**HON. JOCELYN P. TULFO**  
Representative, ACT-CIS PARTYLIST

  
**HON. RALPH WENDEL P. TULFO**  
Representative, 2<sup>ND</sup> DISTRICT OF  
QUEZON CITY



1  
2

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

Twentieth Congress  
First Regular Session

HOUSE BILL NO. 8707

---

Introduced by Representatives JOCELYN P. TULFO and RALPH WENDEL P. TULFO

---

**AN ACT ESTABLISHING THE PHILIPPINE CRITICAL INFORMATION  
INFRASTRUCTURE PROTECTION FRAMEWORK, MANDATING CYBERSECURITY  
STANDARDS FOR VITAL INDUSTRIES, PROVIDING CYBER-DEFENSE GRANTS  
FOR SMALL AND MEDIUM ENTERPRISES, AND APPROPRIATING FUNDS  
THEREOF**

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

1 **SECTION 1. Short Title.** – This Act shall be known as the "Philippine Critical  
2 **Information Infrastructure and Cybersecurity Resilience Act."**

3 **SECTION 2. Declaration of Policy.** – It is the policy of the State to safeguard its digital  
4 sovereignty, protect its citizens' data, and ensure the continuous operation of essential  
5 public and private services. The State recognizes that a secure cyberspace is a  
6 fundamental requirement for economic stability and national security. Therefore, the State  
7 shall proactively fortify its Critical Information Infrastructure (CII) against all forms of cyber  
8 threats, espionage, and digital sabotage.

9 **SECTION 3. Definition of Terms.** – For the purposes of this Act:

- 10 • **(a) Critical Information Infrastructure (CII):** Refers to systems, networks, and  
11 databases, whether physical or virtual, so vital to the Republic of the Philippines  
12 that their incapacitation or destruction would have a debilitating impact on national  
13 security, national economic security, or national public health and safety. This  
14 includes, but is not limited to, the energy, water, telecommunications, banking,  
15 transportation, and healthcare sectors.
- 16 • **(b) Advanced Persistent Threat (APT):** Refers to a prolonged and targeted  
17 cyberattack in which an intruder gains access to a network and remains undetected  
18 for an extended period, often state-sponsored.

19 **SECTION 4. Designation and Protection of Critical Information Infrastructure.** – The  
20 Department of Information and Communications Technology (DICT), in consultation with  
21 the National Security Council (NSC), shall within ninety (90) days from the effectivity of  
22 this Act:

- 23 • **(a)** Identify, classify, and maintain an updated registry of all public and private  
24 entities operating as CII.

- (b) Promulgate mandatory, baseline cybersecurity standards and protocols that all designated CII operators must implement, subject to annual audits by accredited third-party cybersecurity firms.

**SECTION 5. Mandatory Cyber Incident Reporting.** – All designated CII operators and major export-oriented enterprises are mandated to report any verified cybersecurity breach, ransomware attack, or unauthorized network intrusion to the National Computer Emergency Response Team (NCERT) under the DICT within twenty-four (24) hours of discovery. Failure to report within the prescribed period shall result in administrative fines of not less than Five Million Pesos (P5,000,000.00).

**SECTION 6. SME Cybersecurity Grant and Capacity Program.** – Recognizing the vulnerability of the supply chain, the DICT, in coordination with the Department of Trade and Industry (DTI), shall establish a "Digital Shield Grant Program."

The program shall provide financial subsidies and technical assistance to qualified Micro, Small, and Medium Enterprises (MSMEs), particularly those in the export, defense supply, and critical agriculture sectors, to procure verified cybersecurity software, conduct vulnerability assessments, and train personnel.

**SECTION 7. National Cyber Defense Integration.** – The Department of National Defense (DND) and the Armed Forces of the Philippines (AFP) Cyber Group shall establish a joint task force with the DICT to monitor, attribute, and neutralize foreign-based cyber threats and state-sponsored hacking attempts directed at Philippine infrastructure.

**SECTION 8. Appropriations.** – The amount necessary for the initial implementation of this Act shall be charged against the current year's available appropriations of the Department of Information and Communications Technology (DICT), the Department of Trade and Industry (DTI), and other concerned agencies. Thereafter, such sums as may be necessary for the continuous and effective implementation of this Act shall be included in the annual General Appropriations Act.

**SECTION 9. Implementing Rules and Regulations (IRR).** – The DICT, in coordination with the DND, DTI, and the National Privacy Commission (NPC), shall promulgate the necessary rules and regulations for the effective implementation of this Act within sixty (60) days from its approval.

**SECTION 10. Separability Clause.** – If any provision of this Act is declared unconstitutional, the remainder of the Act shall remain in full force and effect.

**SECTION 11. Repealing Clause.** – All laws, presidential decrees, executive orders, and regulations, including specific provisions of Republic Act No. 10844 (DICT Act of 2015), that are inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

**SECTION 12. Effectivity.** – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in at least two (2) newspapers of general circulation.

*Approved,*