

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

TWENTIETH CONGRESS
First Regular Session
House Bill No. 4187



Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT MANDATING CYBER MATURITY AND POSTURE ASSESSMENTS FOR
ALL GOVERNMENT AGENCIES AND OPERATORS OF CRITICAL
INFRASTRUCTURE, AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

The Philippines faces an increasingly hostile cybersecurity environment, with government agencies and private critical infrastructure operators becoming frequent targets of cyberattacks. These threats undermine public trust, disrupt essential services, and compromise sensitive information vital to national security and public welfare.

While cybersecurity policies and frameworks exist, compliance remains inconsistent across agencies and industries. Many government entities and critical sectors lack the capacity to systematically measure their cyber readiness or address vulnerabilities in a timely manner. The absence of a standardized maturity assessment exposes the country to systemic risks and leaves essential infrastructure vulnerable to disruption.

This bill, the “**Cyber Maturity and National Resilience Act**” seeks to institutionalize an annual Cyber Maturity and Posture Assessment (CMPA) for all government agencies and critical infrastructure operators. It requires independent third-party audits, accredited by the Department of Information and Communications Technology (DICT) or internationally recognized certification bodies, to ensure objective evaluation.

The measure also establishes a **National Cybersecurity Accreditation and Ranking System (NCARS)** to promote accountability, transparency, and continuous improvement. By requiring entities to submit Cybersecurity Improvement Plans (CIPs), it ensures vulnerabilities are addressed and national cyber resilience is strengthened.

The proposed law further provides enforcement mechanisms, capacity-building measures, and an initial appropriation to support implementation, particularly for small government agencies and local government units.

In view of the urgent need to strengthen the nation's cyber defenses and resilience, the immediate passage of this bill is earnestly sought.


HON. BRIAN DANIEL POE LIAMANZARES, PhD, MNSA
Representative
FPJ Panday Bayanihan Party-List

Republic of the Philippines
HOUSE OF REPRESENTATIVES

Quezon City, Metro Manila

TWENTIETH CONGRESS

First Regular Session

House Bill No. 4187

Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT MANDATING CYBER MATURITY AND POSTURE ASSESSMENTS FOR
ALL GOVERNMENT AGENCIES AND OPERATORS OF CRITICAL
INFRASTRUCTURE, AND FOR OTHER PURPOSES**

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

SECTION 1. Short Title. — This Act shall be known as the “Cyber Maturity and National Resilience Act.”

SEC. 2. Declaration of Policy. — It is the policy of the State to protect the integrity, confidentiality, and availability of national data, government digital infrastructure, and critical public and private services from cybersecurity threats. To this end, the State shall implement a mandatory cybersecurity assessment and compliance regime to ensure all public agencies and critical sectors meet minimum standards of cyber resilience.

SEC. 3. Coverage. — This Act shall apply to:

- (a) All national government agencies (NGAs), government-owned and controlled corporations (GOCCs), and local government units (LGUs); and
- (b) Operators of critical infrastructure, including but not limited to the following sectors: energy, water, transportation, financial systems, telecommunications, health, public safety, and digital platforms handling citizen data.

SEC. 4. Mandatory Cyber Maturity and Posture Assessments (CMPA). — All covered entities shall:

- (a) Undergo an annual Cyber Maturity and Posture Assessment (CMPA);
- (b) Submit to independent, third-party assessments conducted by accredited cybersecurity audit firms certified by either:
 - (1) the Department of Information and Communications Technology (DICT);
 - (2) a local cybersecurity accrediting body; or
 - (3) an internationally recognized certification authority such as ISO 27001, NIST, or CMMC-certified providers.

The CMPA shall include, among others, an evaluation of:

- (1) Asset inventory and risk management;
- (2) Threat detection and incident response capabilities;
- (3) Access control policies;
- (4) Data protection and encryption standards; and
- (5) Continuity and disaster recovery plans.

SEC. 5. National Cybersecurity Accreditation and Ranking System (NCARS). — The DICT, in coordination with the National Security Council (NSC), shall develop and maintain a National Cybersecurity Accreditation and Ranking System (NCARS) that shall:

- (a) Certify agencies and critical operators at Maturity Levels 1 to 5, based on compliance and capability; and
- (b) Publish an annual public report of rankings, compliance status, and areas of improvement, provided that sensitive details shall be redacted to avoid compromising security.

SEC. 6. Cybersecurity Improvement Plans (CIP). — All covered entities shall:

- (a) Submit a Cybersecurity Improvement Plan (CIP) to the DICT within sixty (60) days of receiving their CMPA report;
- (b) Address major vulnerabilities, outline time-bound actions, and identify required resources; and
- (c) Designate a Cybersecurity Officer or Focal Person accountable for implementation.

SEC. 7. Enforcement and Penalties. — Agencies and operators who fail to comply with CMPA or CIP requirements may be subject to the following penalties:

- (a) Withholding of digital transformation funding, cybersecurity grants, or cloud infrastructure access;
- (b) Suspension of procurement approval for new ICT systems until compliance is achieved;
- (c) Administrative liability for responsible officials under existing civil service rules; and
- (d) For operators of critical infrastructure, license suspension or regulatory penalties under applicable sectoral laws such as those of the ERC, NTC, or BSP.

SEC. 8. Capacity Building and Support. — The DICT shall:

- (a) Maintain a registry of accredited auditors and provide guidance to covered entities;
- (b) Provide technical assistance to LGUs and small government agencies; and
- (c) Develop training modules and maintain a national Cybersecurity Knowledge Hub.

SEC. 9. Appropriations. — The initial amount of Two Hundred Million Pesos (₱200,000,000.00) is hereby appropriated for:

- (a) Establishing the NCARS and the DICT compliance office;
- (b) Subsidizing assessments for small agencies and LGUs; and
- (c) Auditor training and accreditation programs.

Thereafter, appropriations necessary for the implementation of this Act shall be included in the annual General Appropriations Act.

SEC. 10. Implementing Rules and Regulations. — The DICT, in consultation with the NSC, Department of Science and Technology (DOST), Department of Budget and Management (DBM), and private sector experts, shall promulgate the implementing rules and regulations within ninety (90) days from the effectivity of this Act.

SEC. 11. Separability Clause. — If any provision of this Act is declared unconstitutional or invalid, the remaining provisions shall remain in full force and effect.

SEC. 12. Repealing Clause. — All laws, orders, rules, or regulations inconsistent with this Act are hereby repealed or amended accordingly.

SEC. 13. Effectivity Clause. — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in at least two (2) national newspapers of general circulation.

Approved,


HON. BRIAN DANIEL POE LLAMANZARES, PhD, MNSA
Representative
FPJ Panday Bayanihan Party-List