

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

TWENTIETH CONGRESS
First Regular Session
House Bill No. 4186



Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT ESTABLISHING CYBERSECURITY SALARY STANDARDIZATION,
INCENTIVES, AND WORKFORCE DEVELOPMENT PROGRAMS, AND FOR OTHER
PURPOSES**

EXPLANATORY NOTE

The Philippines is increasingly reliant on digital technologies to power its government operations, economic activities, and public services. Along with these advancements, however, comes a surge in cyber threats that endanger national security, disrupt essential services, and compromise sensitive information of citizens and institutions. Recent global and domestic cyber incidents underscore the urgent need for a highly skilled and resilient cybersecurity workforce within the public sector.

Despite the country's progress in establishing cybersecurity policies and infrastructures, the government continues to face significant challenges in attracting and retaining top-tier cybersecurity professionals. Highly trained experts often migrate to the private sector or abroad due to more competitive compensation packages, clearer career growth opportunities, and continuous skill development programs. This talent gap weakens the ability of the State to effectively defend its digital assets against evolving cyber threats.

The proposed measure, the "Cybersecurity Workforce Advancement Act" seeks to address this gap by establishing a comprehensive framework for developing and sustaining a world-class cybersecurity workforce for the Philippine government. Specifically, the bill aims to:

1. Establish a Salary and Career Framework that benchmarks compensation and career progression for government cybersecurity professionals against private sector standards, ensuring competitiveness and merit-based advancement.
2. Implement Strategic Incentives such as bonuses tied to professional certifications, advanced training, and performance-based achievements to encourage continuous skill development.
3. Develop a Talent Pipeline through scholarships, fellowships, and training programs in partnership with academic institutions and the private sector, with service obligations to ensure government benefit.
4. Create a Cybersecurity Reserve Corps composed of private sector and academic experts who may be mobilized during national cyber emergencies to augment government defenses.
5. Provide Adequate Funding through initial and sustained appropriations to guarantee the effectiveness of these initiatives.

By investing in its cybersecurity professionals, the State not only safeguards its digital infrastructure but also ensures the continuity of government services, the protection of critical national assets, and the trust of the Filipino people in the country's digital future.

In view of the foregoing, the immediate passage of this bill is earnestly sought.



HON. BRIAN DANIEL POE LLAMANZARES, 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. 4186

Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT ESTABLISHING CYBERSECURITY SALARY STANDARDIZATION,
INCENTIVES, AND WORKFORCE DEVELOPMENT PROGRAMS, 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 "Cybersecurity Workforce
Advancement Act of 2025."

SECTION 2. Declaration of Policy – It is the policy of the State to proactively secure its digital infrastructure by building a world-class, resilient, and highly skilled cybersecurity workforce within the public sector. The State shall establish a comprehensive framework to attract, recruit, retain, and continuously develop top-tier cybersecurity professionals, including ethical hackers, incident responders, forensic analysts, and security architects, by providing competitive compensation, clear career paths, and robust training programs.

SECTION 3. Objectives – This Act aims to:

- (a) Establish a competitive and transparent salary standardization framework and career progression system for government cybersecurity professionals.
- (b) Implement a robust incentives program that rewards skill development and performance-based achievements.

- (c) Create a sustainable talent pipeline through scholarships, fellowships, and strategic partnerships with academia and the private sector.
- (d) Develop a rapid-response Cybersecurity Reserve Corps to augment government capabilities during national emergencies.

SECTION 4. Cybersecurity Salary and Career Framework – The Department of Budget and Management (DBM), the Civil Service Commission (CSC), and the Department of Information and Communications Technology (DICT) shall collaborate to establish a Cybersecurity Career and Compensation Framework that includes:

- (a) A tiered system of cybersecurity job classifications (e.g., Cybersecurity Analyst I, II, Senior, and Principal).
- (b) Competitive salary grades for these positions, benchmarked against comparable roles in the private sector and with the flexibility to exceed existing salary caps where justified by critical skills or market demand.
- (c) Clear career pathways that define the technical skills, certifications, and experience required for progression from entry-level to leadership roles.

SECTION 5. Promotion and Retention

The CSC shall ensure that:

- (a) Merit-based promotions are prioritized for cybersecurity professionals who demonstrate exceptional performance and acquire advanced skills.
- (b) A performance-based incentive fund is established to provide discretionary bonuses for personnel who exceed performance targets or achieve significant milestones in protecting critical government systems.

SECTION 6. Strategic Certification and Skill Incentives

The DICT shall administer a program that provides:

- (a) Performance-based bonuses for government cybersecurity personnel who obtain and maintain high-value, industry-recognized certifications (e.g., CISSP, OSCP, GIAC). The amount of the bonus shall be tiered and tied to the level and complexity of the certification.
- (b) Reimbursement for certification exam fees and related training costs upon successful completion.
- (c) Priority access to advanced training, workshops, and conferences for certified professionals.

SECTION 7. Cybersecurity Fellowship and Scholarship Programs

The DICT, in collaboration with the Commission on Higher Education (CHED) and the Technical Education and Skills Development Authority (TESDA), shall establish a National Cybersecurity Talent Program that offers:

- (a) Full scholarships for undergraduate and graduate degrees in cybersecurity-related fields, including stipends and book allowances.
- (b) Internship and residency placements within government cybersecurity units (e.g., CERT-PH, DICT's National Cybersecurity Center).
- (c) Recipients of the program must commit to a service obligation of at least two (2) years in a government cybersecurity role for every one (1) year of support received.

SECTION 8. Public-Private Partnerships and the Cybersecurity Reserve Corps

The DICT is authorized to:

- (a) Create a Cybersecurity Reserve Corps comprised of vetted, highly skilled professionals from the private sector and academia who can be called upon for short-term, specialized service during national cyber emergencies or major security incidents.
- (b) Engage in partnerships with private companies and industry organizations to establish mentorship programs, joint training exercises, and knowledge-sharing forums to enhance public sector capabilities.

SECTION 9. Appropriations

An initial amount of ₱1 billion is hereby appropriated for the first year of implementation to fund:

- (a) Salary adjustments, strategic bonuses, and incentives.
- (b) Scholarship, fellowship, and training programs.
- (c) The establishment and operational costs of the Cybersecurity Reserve Corps.
- (d) Subsequent funding shall be included in the annual General Appropriations Act.

SECTION 10. Implementing Rules and Regulations – Within one hundred twenty (120) days of this Act's effectivity, the DICT, DBM, and CSC, in consultation with relevant stakeholders, shall issue the necessary Implementing Rules and Regulations (IRR) to ensure the efficient and effective implementation of this Act.

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

SECTION 12. Repealing Clause – All laws, executive orders, or regulations inconsistent with this Act are hereby repealed or amended accordingly.

SECTION 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,

A handwritten signature in black ink, reading "Brian Poe". The signature is fluid and cursive, with the first name "Brian" and last name "Poe" clearly distinguishable.

HON. BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

Representative

FPJ Panday Bayanihan Party-List