

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City
TWENTIETH CONGRESS
First Regular Session
House Bill No. 2193



Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT INSTITUTIONALIZING A NATIONAL GOVERNMENT ETHICAL
HACKING PROGRAM AND CYBERSECURITY WORKFORCE DEVELOPMENT,
AND APPROPRIATING FUNDS THEREFOR**

EXPLANATORY NOTE

The growing reliance of government agencies on digital systems has brought significant improvements in service delivery and administrative efficiency. However, this increased connectivity also renders our critical information infrastructure more vulnerable to malicious cyber activity. In recent years, public and private institutions in the Philippines have fallen victim to data breaches, ransomware attacks, and other cybersecurity incidents—often resulting in financial loss, compromised citizen data, and reputational harm.

Governments around the world have responded to these threats by collaborating with cybersecurity professionals outside the traditional public sector framework, including independent ethical hackers. Countries such as the United States, through its “Hack the Pentagon” initiative, the United Kingdom via its Ministry of Defence Bug Bounty Program, and Singapore through the Government Bug Bounty Programme (GBBP), have demonstrated the effectiveness of structured, transparent, and legally bounded engagements with accredited cybersecurity researchers. These programs have significantly enhanced the security of national digital assets while fostering the growth of domestic cybersecurity expertise.

This proposed measure, to be known as the “Bug Bounty Act,” institutionalizes a National Government Ethical Hacking Program aimed at identifying and resolving security vulnerabilities in government information systems before they can be exploited. The program

will be administered by the Department of Information and Communications Technology (DICT), in coordination with the Cybercrime Investigation and Coordinating Center (CICC) and the Department of National Defense (DND). It includes the establishment of a centralized vulnerability disclosure platform, the conduct of regular "Hack the Government" events, and a rolling reward system based on the severity and sensitivity of reported bugs. To encourage participation and recognize talent, the program will also offer internship and employment referrals within relevant government agencies.

Recognizing the need for trust and accountability in such a program, all participating ethical hackers must be Filipino citizens who undergo rigorous background checks and accreditation. They must operate strictly within the defined testing scope and under the supervision of responsible government units. Furthermore, the bill guarantees legal protections for ethical hackers acting in good faith and ensures that no criminal or administrative liability shall attach for disclosures made under the program's rules.

Beyond vulnerability testing, this bill invests in long-term cybersecurity capacity building. It mandates the creation of a Philippine Cybersecurity Fellowship Program, offering scholarships and technical training in secure coding, penetration testing, incident response, and digital forensics. In partnership with state universities and colleges (SUCs), TESDA, and private sector partners, the program aims to develop a skilled cybersecurity workforce capable of safeguarding government systems and promoting national digital resilience.

An initial appropriation of ₱100 million is provided for the implementation of the Bug Bounty Program, including the funding of rewards, training, accreditation processes, and infrastructure development. Subsequent appropriations shall be included in the annual General Appropriations Act.

The enactment of this legislation will not only enhance the government's cyber defense capabilities but also foster a culture of responsible disclosure, technical excellence, and civic-minded digital participation. In light of the urgent need to protect our national digital infrastructure, the swift passage of this bill is earnestly sought.

A handwritten signature in black ink, reading "Brian Poe", with a stylized, flowing script.

HON. BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

Representative

FPJ Panday Bayanihan Party-List

Republic of the Philippines
HOUSE OF REPRESENTATIVES

Quezon City

TWENTIETH CONGRESS

First Regular Session

House Bill No. 2193

Introduced by Representative

BRIAN DANIEL POE LLAMANZARES, PhD, MNSA

**AN ACT INSTITUTIONALIZING A NATIONAL GOVERNMENT ETHICAL
HACKING PROGRAM AND CYBERSECURITY WORKFORCE DEVELOPMENT,
AND APPROPRIATING FUNDS THEREFOR**

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 “Bug Bounty Act.”

SECTION 2. Declaration of Policy – It is the policy of the State to strengthen the cybersecurity posture of the Philippine government by leveraging the skills of ethical hackers and cybersecurity professionals to identify and resolve vulnerabilities in government information systems. The State shall also invest in building a robust cybersecurity workforce to protect critical digital infrastructure and uphold national security.

SECTION 3. Definition of Terms

- (a) **Ethical Hacking** – Authorized testing of government digital systems by individuals with technical expertise to identify security flaws, under strict legal and ethical guidelines.

- (b) **Bug Bounty** – A reward or incentive offered for the discovery and responsible disclosure of a security vulnerability in a government system.

(c) **Accredited Ethical Hacker** – A Filipino citizen authorized to participate in government programs under this Act, after passing background checks and obtaining accreditation.

(d) **Critical Government System** – Any information system or platform maintained by a government agency that handles sensitive, classified, or mission-critical data.

SECTION 4. Establishment of the National Government Bug Bounty Program – There is hereby established a National Government Bug Bounty Program, managed by the Department of Information and Communications Technology (DICT), in partnership with the Cybercrime Investigation and Coordinating Center (CICC) and Department of National Defense (DND). The program shall:

(a) Conduct an annual "Hack the Government" event to identify and remediate system vulnerabilities;

(b) Maintain an open rolling bug bounty platform that continuously accepts vulnerability reports on designated government platforms;

(c) Classify rewards based on risk severity and system sensitivity, with bounty amounts ranging from ₱25,000 to ₱500,000;

(d) Provide government job referrals or internship placements for top ethical hackers.

SECTION 5. Accreditation and Background Checks – All participants must:

(a) Be Filipino citizens aged 18 or older;

(b) Pass a National Bureau of Investigation (NBI) and National Intelligence Coordinating Agency (NICA) background check;

- (c) Complete a Code of Ethics and Disclosure Training Program certified by the DICT or DND;
- (d) Sign a non-disclosure agreement (NDA) and participate only within the legally defined testing scope.

SECTION 6. Scope of Testing

The DICT, in consultation with CICC and participating agencies, shall:

- (a) Publish a list of authorized government systems eligible for ethical hacking;
- (b) Define the authorized scope of testing, including prohibited activities (e.g., data theft, denial of service, accessing classified data);
- (c) Maintain a secure vulnerability reporting platform and coordinate real-time communication between hackers and agency technical teams.

SECTION 7. Cybersecurity Training and Workforce Development – To ensure long-term national cyber resilience, the DICT shall:

- (a) Establish the Philippine Cybersecurity Fellowship Program offering full and partial scholarships for students, graduates, and professionals;
- (b) Partner with SUCs, TESDA, and private sector entities to provide:
 - (i) Training in penetration testing, secure coding, digital forensics, and incident response;
 - (ii) Career placements in government cybersecurity roles.

SECTION 8. Protection of Ethical Hackers – No accredited participant shall be prosecuted or penalized for actions taken in good faith, within the approved scope and with proper disclosure,

under this program. Whistleblower protections shall apply to vulnerability disclosures made responsibly through official channels.

SECTION 9. Appropriations – The amount of ₱100 million is hereby appropriated for:

- (a) Bug bounty rewards;
- (b) Development and maintenance of testing platforms;
- (c) Scholarships and training programs;
- (d) Accreditation processes and security vetting.

Subsequent funding shall be included in the General Appropriations Act.

SECTION 10. Implementing Rules and Regulations – Within 90 days of effectivity, the DICT, in coordination with CICC, DND, and NICA, shall promulgate the implementing rules and regulations (IRR) for the enforcement of this Act.

SECTION 11. Separability Clause – If any part or 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, orders, decrees, and regulations inconsistent with this Act are hereby repealed or modified accordingly.

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

Approved,



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