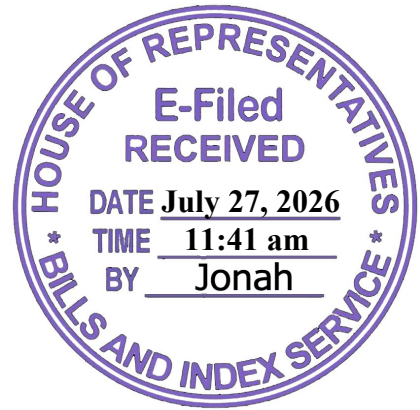


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10236



Introduced by **HON. JERRY EVANGELISTA PEREZ**

**AN ACT ESTABLISHING THE PHILIPPINE NATIONAL POLICE CYBERSECURITY
OPERATIONS CENTER FOR THE PROTECTION OF PNP CRITICAL
INFORMATION INFRASTRUCTURE, DEFINING ITS POWERS AND FUNCTIONS,
APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

The Philippine National Police (PNP) increasingly relies on digital systems, interconnected networks, electronic databases, and online frontline services in performing its law-enforcement and public-safety functions. While these technologies have improved the delivery of police services, they have also exposed the organization to cyberattacks, unauthorized access, data breaches, malware, service disruptions, and other forms of cyber intrusion.

A successful attack against PNP systems may interrupt essential police operations, compromise sensitive and special personal information, impair the delivery of public services, and weaken public confidence in law-enforcement institutions. The reported breach involving the PNP Firearms and Explosives Office illustrates the serious consequences that may arise when systems containing sensitive government and citizen information are not adequately protected.

Cybersecurity within the PNP can no longer be treated solely as a routine information technology function. It is an essential component of operational readiness, data protection, public safety, and national security. The protection of PNP Critical Information Infrastructure must therefore be supported by a permanent, specialized, and coordinated institutional capability.

This measure seeks to establish the PNP Cybersecurity Operations Center, or PNP CSOC, as the primary operational and technical unit of the PNP responsible for cybersecurity operations, cyber threat intelligence, and incident response for the protection of PNP Critical Information Infrastructure. It is consistent with the declared policy of the State to strengthen the cybersecurity posture of law-enforcement agencies and ensure the security, integrity, confidentiality, and availability of PNP systems and online frontline services.

The PNP CSOC will provide a centralized mechanism for continuously monitoring cyber threats, identifying vulnerabilities and emerging attack methods, analyzing cybercrime trends that may affect PNP systems, and coordinating timely responses to significant cybersecurity incidents. Instead of relying on fragmented or purely reactive measures, the Center will allow the PNP to adopt a unified and proactive approach to the protection of its digital assets and critical systems.

The Center will also provide specialized technical and digital forensic support to PNP units investigating cybercrime offenses that directly affect, or originate from attacks against, PNP Critical Information Infrastructure. This includes the proper identification, collection, examination, preservation, and handling of digital evidence necessary to support investigations and prosecutions.

In addition, the PNP CSOC will gather, analyze, and disseminate actionable cyber threat intelligence; develop cybersecurity, incident-response, and digital-forensics training programs for PNP personnel; conduct research and development; recommend appropriate cybersecurity policies to the Chief PNP; and contribute to public-awareness initiatives on the protection of personal information when using PNP online services. It will likewise coordinate with the Department of Information and Communications Technology and other relevant national and international government and law-enforcement institutions involved in cybersecurity and the protection of government-owned critical infrastructure.

The mandate of the PNP CSOC is deliberately focused on the protection of PNP Critical Information Infrastructure. It is not intended to replace or duplicate the general mandates of existing cybersecurity and cybercrime agencies. Rather, it will strengthen the PNP's internal capability while enabling more effective coordination with other government institutions whenever a cyber incident affects PNP systems, networks, databases, or digital services.

To ensure effective leadership and accountability, the Center will be headed by a Director with the rank of Police Brigadier General or higher and will be composed of highly skilled and specialized personnel, including cybersecurity analysts, cybercrime investigators, and digital forensic examiners. Its detailed organizational structure, staffing pattern, and regional presence will be determined by the Chief PNP, in consultation with the National Police Commission and subject to the availability of funds.

The measure further directs the PNP to provide the Center with the technologies, tools, secure infrastructure, digital forensic laboratories, and incident-response capabilities necessary to perform its functions. Because the Center will handle sensitive cybersecurity and investigative information, the bill requires the strictest confidentiality and the adoption of safeguards against unauthorized access, use, disclosure, or compromise.

Funding for the establishment, continuous operation, and enhancement of the PNP CSOC shall be included in the annual General Appropriations Act and the regular budget of the PNP. The Chief PNP, in coordination with the National Police Commission and the Department of Information and Communications Technology, shall promulgate the necessary implementing rules and regulations within ninety days from the effectivity of the proposed law.

The establishment of the PNP Cybersecurity Operations Center will institutionalize a dedicated, professional, and unified cybersecurity capability within the Philippine National Police. It will strengthen the protection of PNP Critical Information Infrastructure, safeguard sensitive government and citizen data, improve the resilience and continuity of police operations, and enhance the PNP's capacity to prevent, detect, investigate, and respond to cyber threats.

As law enforcement becomes increasingly dependent on digital technologies, the PNP must be equipped not only to police the physical domain but also to protect the digital systems upon which its operations and public services depend.

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



JERRY EVANGELISTA PEREZ
2nd District, City of Zamboanga

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10236

Introduced by **HON. JERRY EVANGELISTA PEREZ**

**AN ACT ESTABLISHING THE PHILIPPINE NATIONAL POLICE CYBERSECURITY
OPERATIONS CENTER FOR THE PROTECTION OF PNP CRITICAL
INFORMATION INFRASTRUCTURE, DEFINING ITS POWERS AND FUNCTIONS,
APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES**

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

SEC. 1. Title. – This Act shall be known as the "PNP Critical Information Infrastructure Cybersecurity Act."

SEC. 2. Declaration of Policy. – It is hereby declared the policy of the State to strengthen the cybersecurity resilience of the Philippine National Police (PNP) and ensure the protection of its Critical Information Infrastructure (CII), which is essential to the effective delivery of law enforcement services, the preservation of public trust, and the safeguarding of national security interests. The State recognizes that the confidentiality, integrity, availability, and resilience of PNP information systems, digital platforms, databases, communications networks, and online frontline services are indispensable to the maintenance of peace and order and the protection of sensitive government and citizen information.

Toward this end, the State shall establish a dedicated and specialized cybersecurity capability within the PNP to provide continuous cyber threat monitoring, cyber threat intelligence, incident detection and response, digital forensics, and cybersecurity risk management for PNP Critical Information Infrastructure. Such capability shall enable the PNP to anticipate, prevent, detect, investigate, and respond to evolving cyber threats, cyberattacks, unauthorized access, data breaches, and other malicious activities that may compromise its operations and information assets.

The State further recognizes that emerging cyber threats increasingly transcend the digital domain and may have direct implications for public safety, including the misuse of online platforms to facilitate malicious activities, disseminate threats, target vulnerable sectors, and influence harmful real-world conduct. Accordingly, the PNP shall be equipped with the necessary institutional, technical, and operational capabilities to address these evolving risks while ensuring the protection of personal data, digital evidence, and other sensitive information entrusted to the government.

In pursuing these objectives, the State shall promote inter-agency cooperation, capacity development, technological innovation, and international collaboration to enhance the PNP's cybersecurity posture and ensure the continued security, reliability, and resilience of its critical information infrastructure.

SEC. 3. Establishment of the PNP Cybersecurity Operations Center. – There is hereby established the Philippine National Police Cybersecurity Operations Center (PNP CSOC), which shall serve as the PNP's central cybersecurity command, operations, and coordination hub for the protection of PNP Critical Information Infrastructure (CII).

The PNP CSOC shall be the primary operational and technical unit responsible for safeguarding PNP information systems, digital platforms, databases, communications networks, digital assets, and other critical cyber resources against cyber threats, cyberattacks, unauthorized access, data breaches, malicious online activities, and other cybersecurity risks. It shall maintain a continuous capability to monitor, detect, analyze, prevent, mitigate, and respond to incidents that may compromise the confidentiality, integrity, availability, and resilience of PNP information infrastructure.

As the focal point for cybersecurity operations within the PNP, the PNP CSOC shall integrate cybersecurity monitoring, cyber threat intelligence, incident response, digital forensics, vulnerability management, risk assessment, and cyber defense operations into a unified framework for the protection of PNP Critical Information Infrastructure.

The PNP CSOC shall serve as the principal center for the collection, processing, analysis, and dissemination of cyber threat intelligence relevant to the PNP. It shall identify emerging cyber threats, threat actors, attack methodologies, vulnerabilities, indicators of compromise, online extremist activities, and other cyber-enabled risks that may affect PNP operations, public safety, or national security. Through strategic, operational, and tactical threat intelligence, the Center shall provide timely warnings, risk assessments, and actionable recommendations to support informed decision-making, incident prevention, cybersecurity planning, and operational readiness across all PNP units.

The Center shall likewise establish mechanisms for information sharing and threat intelligence exchange with relevant government agencies, the cybersecurity and law enforcement community, critical infrastructure operators, academic institutions, private sector partners, and international counterparts, subject to applicable laws, regulations, and security protocols. Such collaboration shall enhance the PNP's ability to anticipate evolving threats, strengthen cyber resilience, and support whole-of-government efforts to address cyber-enabled crimes and emerging digital risks.

The PNP CSOC shall operate as a specialized and proactive capability designed to strengthen the PNP's cyber defense posture, protect sensitive government and citizen information, preserve public trust in digital services, support law enforcement operations, and contribute to the maintenance of public safety and national security in an increasingly interconnected and technology-driven environment.

SEC. 4. Mandate and Functions. – The PNP Cybersecurity Operations Center (PNP CSOC) shall serve as the Philippine National Police's central cybersecurity operations, threat intelligence, and cyber defense capability for the protection of PNP Critical Information Infrastructure (CII). In pursuit of its mandate, it shall perform the following functions:

- (a) Security Operations and Continuous Monitoring – Establish and maintain a centralized capability for the continuous monitoring, detection, analysis, and management of cybersecurity events affecting PNP information systems, networks, digital platforms, databases, communications infrastructure, and other critical cyber assets. The Center shall identify vulnerabilities, indicators of compromise, malicious activities, and emerging attack vectors to enable timely preventive and corrective actions.
- (b) Cyber Threat Intelligence – Collect, process, analyze, produce, and disseminate strategic, operational, and tactical cyber threat intelligence relevant to the PNP. The Center shall monitor emerging threats, threat actors, cybercriminal networks,

- malicious online activities, extremist and radicalization trends in digital spaces, vulnerabilities, and cyber-enabled risks that may affect law enforcement operations, public safety, or national security. It shall provide actionable intelligence, early warning advisories, threat assessments, and cybersecurity recommendations to support decision-making, operational readiness, and risk mitigation across all PNP units.
- (c) **Cybersecurity Incident Response and Recovery** – Serve as the PNP's lead operational unit for the management, containment, investigation, remediation, and recovery of cybersecurity incidents affecting PNP Critical Information Infrastructure. The Center shall coordinate with relevant government agencies, service providers, and stakeholders to ensure a timely, effective, and coordinated response to cyber incidents and security breaches.
 - (d) **Digital Forensics and Cyber Investigation Support** – Provide specialized technical assistance, cyber forensic capabilities, malware analysis, digital evidence collection, preservation, examination, and related investigative support to PNP units in connection with cybercrime investigations, cyber-enabled offenses, and incidents affecting PNP systems and information assets.
 - (e) **Vulnerability Assessment and Cyber Risk Management** – Conduct cybersecurity assessments, penetration testing, security audits, vulnerability analyses, and risk assessments of PNP information systems and critical infrastructure. The Center shall develop and recommend appropriate safeguards, controls, and mitigation measures to strengthen cyber resilience and reduce risk exposure.
 - (f) **Cyber Defense and Infrastructure Protection** – Develop, implement, and oversee technical and operational measures necessary to protect PNP Critical Information Infrastructure from cyberattacks, unauthorized access, data loss, disruption, sabotage, and other threats that may compromise the confidentiality, integrity, availability, or resilience of PNP systems and services.
 - (g) **Information Sharing and Inter-Agency Coordination** – Establish and maintain cybersecurity cooperation, threat intelligence-sharing arrangements, and operational coordination with the Department of Information and Communications Technology (DICT), the Cybercrime Investigation and Coordinating Center (CICC), other government agencies, law enforcement organizations, critical infrastructure operators, private sector partners, academic institutions, and international counterparts, subject to applicable laws, regulations, and security protocols.
 - (h) **Capacity Building and Professional Development** – Develop and implement training, certification, simulation, and professional development programs to enhance the cybersecurity competencies, cyber investigation capabilities, digital forensic expertise, and incident response readiness of PNP personnel.
 - (i) **Research, Innovation, and Technology Development** – Conduct and support research, innovation, and technology development initiatives relating to cybersecurity, cyber defense, digital forensics, artificial intelligence, threat detection, and other emerging technologies to strengthen the operational effectiveness of the PNP's cybersecurity capabilities.

- (j) Policy Development and Strategic Advisory Services – Provide strategic advice and recommendations to the Chief, PNP on cybersecurity policies, standards, governance frameworks, operational procedures, and long-term cyber resilience strategies necessary to protect PNP Critical Information Infrastructure.
- (k) Cybersecurity Awareness and Stakeholder Engagement – Support public awareness, cyber hygiene education, and stakeholder engagement initiatives aimed at promoting responsible use of digital technologies, protecting personal information, combating cyber-enabled threats, and enhancing public confidence in PNP digital services.
- (l) Such Other Functions – Perform such other cybersecurity-related functions as may be assigned by the Chief, PNP or provided by law, consistent with the mandate of protecting PNP Critical Information Infrastructure and strengthening the cyber resilience of the Philippine National Police.

SEC. 5. Organizational Structure. – The PNP Cybersecurity Operations Center (PNP CSOC) shall be headed by a Director, with the rank of Police Brigadier General or higher, who shall be appointed by the Chief, Philippine National Police (PNP), and who shall possess demonstrated competence, experience, and training in cybersecurity, information and communications technology, intelligence, cybercrime investigation, digital forensics, or related fields.

The PNP CSOC shall be organized as a specialized, multidisciplinary, and mission-oriented unit composed of uniformed and non-uniformed personnel with expertise in cybersecurity operations, cyber threat intelligence, digital forensics, cyber defense, incident response, cybercrime investigation, network security, data analytics, information technology, risk management, research and development, and other relevant disciplines necessary to fulfill its mandate.

To ensure continuous and effective cyber defense operations, the PNP CSOC shall establish and maintain functional divisions, units, or teams responsible for, among others:

- a. Security Operations and Continuous Monitoring;
- b. Cyber Threat Intelligence and Analysis;
- c. Cybersecurity Incident Response and Recovery;
- d. Digital Forensics and Cyber Investigation Support;
- e. Vulnerability Assessment and Cyber Risk Management;
- f. Cyber Defense and Infrastructure Protection;
- g. Research, Innovation, and Emerging Technologies;
- h. Training, Capacity Building, and Cybersecurity Awareness; and
- i. Strategic Planning, Policy Development, and Inter-Agency Coordination.

The PNP CSOC shall operate on a continuous basis and maintain the necessary personnel, facilities, technologies, and operational capabilities to provide real-time cyber monitoring, threat detection, intelligence analysis, incident response, and cyber defense support for PNP Critical Information Infrastructure.

Subject to the availability of funds and the operational requirements of the PNP, the Chief, PNP, in consultation with the National Police Commission (NAPOLCOM), may establish regional, provincial, or other field-based cybersecurity units or satellite operations centers to enhance the nationwide cyber resilience, threat visibility, and incident response capabilities of the PNP.

The Chief, PNP, in consultation with NAPOLCOM and other relevant government agencies, shall determine the detailed organizational structure, staffing pattern, qualification

standards, and operational framework of the PNP CSOC, taking into consideration international best practices, evolving cyber threats, and the long-term cybersecurity requirements of the Philippine National Police.

This provision shall be interpreted to ensure that the PNP CSOC develops into a professional, intelligence-driven, and technology-enabled organization capable of proactively protecting PNP Critical Information Infrastructure and supporting the broader objectives of public safety, law enforcement effectiveness, and national security in the digital age.

SEC. 6. Powers of the Director. – The Director of the PNP Cybersecurity Operations Center (PNP CSOC) shall exercise leadership, supervision, and operational control over the Center and shall be responsible for the effective implementation of its mandate. For this purpose, the Director shall have the authority to:

- a. Provide strategic direction, oversight, and management of the PNP CSOC and ensure the continuous and effective performance of its cybersecurity operations, cyber defense, threat intelligence, incident response, and critical infrastructure protection functions;
- b. Formulate, issue, implement, and enforce policies, standards, guidelines, operational procedures, and cybersecurity frameworks necessary to strengthen the security, resilience, and protection of PNP Critical Information Infrastructure, subject to existing laws, regulations, and approval requirements;
- c. Direct and coordinate the conduct of cybersecurity monitoring, cyber threat intelligence activities, risk assessments, vulnerability management, digital forensics operations, and incident response measures to address actual or emerging threats affecting PNP information systems and digital assets;
- d. Establish and maintain mechanisms for information sharing, threat intelligence exchange, operational coordination, and collaborative cybersecurity initiatives with government agencies, law enforcement organizations, critical infrastructure operators, academic institutions, private sector partners, and international counterparts, subject to existing laws and with the approval of the Chief, PNP, where required;
- e. Recommend, develop, and implement programs, projects, technologies, and capability-enhancement initiatives necessary to improve the cyber resilience, operational readiness, and technological capabilities of the PNP;
- f. Administer, allocate, and manage the personnel, financial, technological, and other resources of the PNP CSOC in accordance with existing laws, government accounting and auditing rules, and established PNP policies;
- g. Recommend the appointment, assignment, promotion, training, professional development, recognition, and disciplinary action of personnel assigned to the PNP CSOC, in accordance with applicable laws, rules, and regulations;
- h. Represent the PNP on matters relating to cybersecurity operations, cyber defense, cyber threat intelligence, and critical information infrastructure protection before national, regional, and international forums, subject to existing laws and policies;
- i. Submit periodic reports and strategic assessments to the Chief, PNP on the cybersecurity posture of the organization, significant cyber incidents, emerging threats, operational performance, capability requirements, and other matters relevant to the protection of PNP Critical Information Infrastructure; and
- j. Exercise such other powers and perform such other functions as may be necessary, incidental, or related to the attainment of the objectives of this Act, or as may be assigned by the Chief, PNP, consistent with law.

The Director shall ensure that the PNP CSOC operates as an intelligence-driven, technology-enabled, and proactive cybersecurity organization capable of anticipating, preventing, detecting, and responding to evolving cyber threats in support of public safety, law enforcement effectiveness, and national security.

SEC. 7. Technical Expertise and Equipment. – The PNP shall ensure that the PNP CSOC is equipped with state-of-the-art technologies, tools, and infrastructure necessary to carry out its

functions effectively. This includes, but is not limited to, advanced digital forensic laboratories, secure network infrastructure, and incident response tools specifically for the protection of PNP-CII.

SEC. 8. Confidentiality of Information. – All information obtained by the PNP CSOC in the course of its duties, particularly sensitive data related to the cybersecurity of PNP-CII and investigations thereof, shall be treated with the strictest confidentiality and shall not be disclosed to unauthorized persons or entities, except as may be required by law or lawful court order. Appropriate safeguards shall be put in place to protect such information.

SEC. 9. Appropriations. – The amount necessary to carry out the provisions of this Act shall be included in the annual General Appropriations Act. Thereafter, such sums as may be necessary for the continuous operation and enhancement of the PNP CSOC shall be included in the annual budget of the Philippine National Police.

SEC. 10. Implementing Rules and Regulations. – Within ninety (90) days from the effectivity of this Act, the Chief PNP, in coordination with the National Police Commission (NAPOLCOM), the Department of Budget and Management (DBM), the Department of Interior and Local Government (DILG), and the Department of Information and Communications Technology (DICT), shall promulgate the necessary implementing rules and regulations for the effective implementation of this Act.

SEC. 11. Separability Clause. – If any provision of this Act is declared unconstitutional or invalid, the other provisions not affected thereby shall remain in full force and effect.

SEC. 12. Repealing Clause. – All laws, decrees, executive orders, rules and regulations, and other issuances or parts thereof which are inconsistent with this Act are hereby repealed or modified accordingly.

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

Approved.