

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
Third Regular Session

House Bill No. **11191**



Introduced by **HON. ROBERT ACE S. BARBERS**

EXPLANATORY NOTE

The accelerated global adoption of digital technologies has brought undeniable benefits, transforming industries and creating new opportunities for economic growth and social development. However, this digital shift has also led to an alarming rise in cybercrimes, including ransomware attacks, financial fraud, identity theft, and cyberterrorism. The Philippines is not immune to this phenomenon, as evidenced by significant incidents that threaten national security, economic stability, and public safety.

The Philippine Health Insurance Corporation (PhilHealth) ransomware attack in 2023 illustrates the escalating sophistication and frequency of cyber threats. The cybersecurity firm *Kaspersky* reports that the Philippines experienced over 15,312 attempted ransomware attacks against businesses in 2023 alone, making it the fourth most targeted nation in Southeast Asia. Furthermore, the misuse of emerging technologies, such as artificial intelligence (deepfakes) and cryptocurrency, has compounded these threats. These tools have been exploited to spread misinformation, commit fraud, and evade law enforcement, undermining public trust and destabilizing critical institutions.

The Cybercrime Investigation and Coordinating Center (CICC), created under Republic Act No. (RA) 10175, the "Cybercrime Prevention Act of 2012," is tasked to coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities. While the CICC, an inter-agency body, has made strides in fulfilling its mandate, its current resources and capabilities remain inadequate to address the rapid evolution and increasing volume of cybercrimes. Further, certain measures in subsequent laws such as RA 10844, which transferred CICC's cybersecurity mandate to the Department of Information and Communications Technology (DICT), need to be revisited. It is firmly submitted that placing cybersecurity and cybercrime prevention and suppression under one roof, i.e., CICC, will enhance coordination of the two distinct technical fields, foster joint incidence response, and leverage fully the use of shared technologies, which are critical in ensuring data and system protection and real-time collaboration and faster response time. Thus, there is pressing need to restore the cybersecurity mandate of CICC as originally designed.

Under RA 10175, the CICC is to lead and coordinate efforts to prevent and suppress cybercrime, yet its lack of investigative powers, such as subpoena authority, has severely limited its effectiveness. Meanwhile, RA 10973 granted similar powers to

select officials of the Philippine National Police (PNP), recognizing the need for swift evidence-gathering in complex investigations. Cybercrimes—ranging from ransomware to financial fraud—demand immediate action to secure volatile digital evidence, which the CICC, with its specialized expertise, is uniquely equipped to handle. Without subpoena powers, however, the CICC is unable to swiftly compel the production of critical evidence, resulting in delays that perpetrators exploit.

Further, considering that cybersecurity and digital forensics require highly technical and specialized skills, talent acquisition and development are critical. Needless to say, competitive compensation package and continuing top-of-the-line training of the staff are essential to keep the country's cybersecurity and crime prevention and suppression agency robust and relevant.

Given the acute limitations of the Salary Standardization Law (SSL) in attracting cyber talents, exemption of CICC from the SSL cannot be seriously opposed. Further, enough resources, given the rapidly evolving technology and risks growing in sophistication each day, must be committed for continuing staff training.

Specifically, this bill proposes to:

- Streamline CICC's governance structure;
- Rationalize roles of agency participants therein to avoid duplication and leverage the information technology-based competence of CICC;
- Grant subpoena powers to the CICC Executive Director to ensure that ephemera digital evidence is swiftly gathered or preserved;
- Restore CICC's cybersecurity mandate;
- Institutionalize the multi-stakeholder and collaborative National Anti-Cybercrime Hub (NACH);
- Set out as policy the continuing build up of cybersecurity and cybercrime capability; and
- Attract and maintain the best cybersecurity and anti-cybercrime talent.

The proposed measures are vital to securing a safe and resilient digital environment for the Philippines, safeguarding its sovereignty, and promoting public trust in the digital space.

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

REP. ROBERT ACE S. BARBERS
2nd District, Surigao del Norte



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
Third Regular Session

HOUSE BILL NO. 11191

Introduced by **HON. ROBERT ACE S. BARBERS**

AN ACT
RATIONALIZING AND STRENGTHENING THE PHILIPPINE CYBERSECURITY
POSTURE AND CYBERCRIME RESPONSE

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

Section 1. Streamlining of the Cybercrime Investigation and Coordinating Council (CICC) governance structure and roles. – As an amendment to Sec. 25 of RA 10175, the CICC, under Republic Act No. (RA) 10175, shall have the governance structure as follows: the Department of Information and Communications Technology (DICT) Secretary as Chairperson and the Executive Director of the CICC as Vice-Chairperson. The members thereof shall be: the Director of the National Bureau of Investigation (NBI), the Chief of the Philippine National Police (PNP), the Head of the Department of Justice-Office of Cybercrime (DOJ-OOC), and one (1) representative each from the private sector and the academe.

There shall be an Executive Committee headed by the Executive Director with the rank of Undersecretary and duly designated representatives of the NBI, PNP, and the DOJ-OOC.

Section 2. Rationalization of roles and functions in the CICC. – The CICC shall coordinate the efforts of law enforcement authorities in enforcing the provisions of RA 10175 and this Act.

Further, an operations center shall be established within the CICC composed of organic CICC staff which shall be under the direct control and supervision of the Executive Director: Provided, that the Executive Director may also request participating agencies to assign or detail selected personnel or representative to CICC or its specialized facilities, programs, projects or initiatives, to make up the secretariat or operating teams, as may be warranted.

The DOJ-OOC shall be the central authority in all matters related to international mutual legal assistance and extradition relative to cybercrimes.

Section 3. Subpoena powers. – The Executive Director of the CICC shall have the authority to administer oaths and to issue subpoena ad testificandum and subpoena duces tecum in connection with investigations conducted by the CICC.

Provided, however, that such authority shall be exercised exclusively by the Executive Director and shall not be delegated to any other person or office.

A subpoena shall clearly state the nature and purpose of the investigation, and in the case of a subpoena duces tecum, it shall also contain a reasonable and specific description of the books, documents, electronic data, digital files, or other materials required to be produced, which must be relevant and material to the investigation.

Non-compliance with a duly issued subpoena ad testificandum or subpoena duces tecum shall constitute grounds for the filing of an action for indirect contempt under the Rules of Court, which shall be filed with the appropriate Regional Trial Court.

Section 4. Restoration of cybersecurity mandate. – As an amendment to Sec. 15 (3) of RA 10844, all powers and functions related to cybersecurity including, but not limited to the formulation of the National Cybersecurity Plan, the establishment and operation of the National Computer Emergency Response Team (CERT), and the facilitation of international cooperation on intelligence regarding cybersecurity matters, which were previously transferred to the DICT, shall revert to the CICC, including CERT's assets and personnel.

The Cybersecurity Bureau of the DICT shall primarily perform policy formulation and development relative to cybersecurity. The CICC shall be the lead agency in hardening the country's cybersecurity posture and responding to cyber threats and incidents.

Section 5. Institutionalization of the National Anti-Cybercrime Hub (NACH). – The NACH, under the CICC's administration, shall be institutionalized to support cybercrime prevention and suppression, foster the public's cyber safety, and protect the integrity of the country's digitalization.

The NACH shall be situated and maintained in a strategic location in a government property given the sensitive and critical nature of its tasks and assets.

The CICC shall ensure that the NACH adequately meets the relevant international standards for such kind of facility, adopts best practices, engages relevant and specialized human resource requirements, and acquires/gains access to the necessary equipment, and tools.

Section 6. Continuing authority to build up cybersecurity and cybercrime capability. – The CICC shall institute a program that will train, develop, and expand the ranks, as well as, build up expertise of professionals essential in cybersecurity and cybercrime response. It shall leverage existing expertise from the government, industry, and the academe for course development and program implementation.

Section 7. Authority to re-organize CICC. – Subject to Civil Service and budget laws, rules, and regulations, the CICC is hereby authorized to formulate and implement the necessary re-organization plans and activities. The name of the positions and description of qualification standards relating to the new table of organization shall take into account the technical nature thereof including the reasonable compensation level as prevailing in the sector, among others. The

Department of Budget and Management (DBM) shall actively assist CICC in preparing such a reorganization plan, and expedite the processing of the plan and funding thereof to support the same.

Section 8. Compensation and Other Emoluments for CICC officials and personnel. – To ensure that the CICC may attract the necessary expertise and talents given its highly technical mandate, the compensation and other emoluments of its officials and personnel shall be exempted from the coverage of RA No. 6758, otherwise known as the “Salary Standardization Act.” For this purpose, their salaries and emoluments shall be set based on an objective classification system, taking into consideration the highly specialized nature of, importance, and responsibilities attached to the respective positions, and shall be submitted to the President of the Philippines for his approval.

Section 9. Support from government agencies. – All heads of departments, bureaus, offices, agencies, and instrumentalities of the national government, including officials of the local governments, are directed to support the CICC in the formulation and implementation of plans, programs, activities, and projects geared towards fostering cybersecurity and effectively combating cybercrime.

Section 10. Separability. – If any provision of this Act is declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

Section 11. Repeal. – All laws, decrees, orders, issuances, rules, and regulations, or other issuances or parts thereof 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 any two (2) newspapers of general circulation in the Philippines.

Approved,