Republic of the Philippines
House of Representatives

HOUSE OF REPRESENTATIVES
E-Filed
RECEIVED
DATE August 20, 2024
TIME 2:19 pm
BY Reli
BILLS AND INDEX SERVICE

19th CONGRESS
Third Regular Session

HOUSE BILL NO. 10797

Introduced by Hon. Charisse Anne Hernandez
Lone District of Calamba, Province of Laguna

EXPLANATORY NOTE

"Amidst the accelerating tempo of technology progress and a vastly interconnected global landscape, the Philippines emerges as a pivotal player with a capacity to transform into a digitally advanced nation. But in order to fully realize these developments, it is imperative that we also give our utmost attention to its many accompanying challenges.

Guided by strong developmental principles, the National Cybersecurity Plan 2024-2029 of the Department of Information and Communications Technology aims to position the country at the cutting edge of the digital age. ***By reinforcing our cybersecurity defense strategies, we prepare ourselves for the imminent risks that come with these new advancements.***

As we look towards the future, I urge all government agencies, the private sector, and citizens to continue to work together in creating a secure digital environment for everyone. United as one, let us place trust, accountability, and transparency at the forefront of our collective endeavors so that we can move forward with courage and determination as we shape the future and leave a lasting impact on the work stage. Together, let us make the Philippines rise to its fullest potential."

Ferdinand R. Marcos Jr.,
President
Republic of the Philippines
National Cybersecurity Plan 2023-2028
Department of Information and Communications Technology

In line with the call of the President to work together in creating a secure digital environment

for everyone and with the urgent call of the legislators to investigate into the alleged massive data breach and cyberattacks on government's databases, on April 30, Tuesday, the Committee on Information and Communications Technology, together with the Committee on Public Information and the Committee on Public Order and Safety, conducted an investigation in aid of legislation concerning the integrity of our country's cybersecurity, particularly the series of hacking and data leakage of personal information from our government's databases. The agenda included:

1. HR 931 – Investigation into the alleged massive data breach of the records of the Philippine National Police, National Bureau of Investigation, Bureau of Internal Revenue, Special Action Force Operations Management Division, and Civil Service Commission introduced by Rep. France Castro.
2. HRs 1350, 1389, 1402 & 1408 – Investigation into the Medusa ransomware cyber-attack on Philippine Health Insurance Corp. (PhilHealth) and the leak of personal records of PhilHealth employees and members introduced by Reps. Arlene Brosas, Bienvenido Abante Jr., ZiaurRahman 'Zia' Alonto Adiong, and Bryan Revilla.
3. HR 1387 – Urging the Department of Information and Communications Technology (DICT) to conduct a governmentwide cybersecurity audit, in light of the continuous proliferation and alarming trend of cyberattacks against the government and private firms in the country, and to summon the DICT to submit the report of this audit to Congress, with the end in view of determining the remedial legislation needed to strengthen our existing cybersecurity policies and laws introduced by Rep. Wilbert Lee.
4. HR 1392 – Investigation into determining the extent of the risks to government institutions and the data privacy of Filipino citizens due to the recent cyberattacks on the Philippine Statistics Authority and the House of Representatives, and to institute vital measures to bolster our national digital defenses introduced by Minority Leader Marcelino Libanan.
5. HR 1583 – Investigation into the series of cyber-attacks involving government agencies introduced by Rep. Charisse Anne Hernandez.
6. HR 1610 – Investigation into the hacking and data leakage of personal information of the databases of the Department of Education, DICT, and other government agencies in violation of the Data Privacy Act, Cybercrime Prevention Act, and other pertinent laws introduced by Rep. Raoul Danniel Manuel.

The committee highlighted significant concerns, including the lack of coordination among different agencies, the lack of capability to apprehend offenders outside the country, and the failure to prosecute even when perpetrators were identified. Furthermore, the committees urged lawmakers to legislate for the country's cybersecurity defense system in line with President Ferdinand R. Marcos Jr.'s approval of the National Cybersecurity Plan 2024-2029. This defense plan aims to provide policy direction and operational guidelines for building a robust cybersecurity posture and fortifying the country's cyberspace against online threats.

The cybersecurity landscape in the Philippines faces several challenges and issues, particularly concerning government agencies. Some key problems identified include:

1. Lack of Comprehensive Legislation: There's a need for more robust cybersecurity laws and regulations tailored to modern threats and technologies. Existing laws like the Cybercrime Prevention Act of 2012 may not fully cover emerging cyber threats, prosecution of offenders, and cybersecurity defense systems.

2. Insufficient Funding and Resources: Many government agencies struggle with limited budgets allocated for cybersecurity initiatives, hindering their ability to implement robust cybersecurity measures and acquire advanced technologies.
3. Skills Shortage and Capacity Building: There is a shortage of skilled cybersecurity professionals within government agencies. Training and capacity-building programs are essential to enhance the capabilities of existing personnel.
4. Fragmented Coordination: Coordination among various government agencies responsible for cybersecurity (such as the Department of Information and Communications Technology, National Privacy Commission, and National Cybersecurity Coordination Center) can be fragmented, leading to gaps in threat intelligence sharing and response.
5. Dependency on Legacy Systems: Some government agencies still rely on outdated IT infrastructure and systems, which are more vulnerable to cyber-attacks due to a lack of regular updates and security patches.
6. Rising Cyber Threats: The Philippines faces increasing cyber threats, including phishing attacks, ransomware, and data breaches targeting both government agencies and private sectors. These threats evolve rapidly and require continuous adaptation of cybersecurity strategies.
7. Limited Public Awareness: There is a need for enhanced public awareness campaigns to educate government personnel and citizens about cybersecurity best practices, such as strong password management and recognizing phishing attempts.
8. Regulatory Compliance: Compliance with cybersecurity standards and regulations is often challenging for government agencies, particularly smaller ones and remote offices with limited resources to meet stringent requirements.

Addressing these challenges requires a multi-faceted approach, including legislative reforms, increased investment in cybersecurity infrastructure and personnel, enhanced coordination among agencies, and public-private partnerships to strengthen the overall cybersecurity ecosystem in the Philippines.

Moreover, in light of the recent news of the illegal activities of the Philippine Offshore Gaming Operators (POGOs) industry, Philippine government officials and legislators have on many occasions called for the shutdown of POGOs due to the whole gamut of criminalities involving the same.

The Cybercrime Investigation and Coordinating Center (CICC) is bracing for the continued proliferation of online scams with the rise of the so-called scam hubs, which are allegedly former gaming operators of POGOs. On the watch of President Marcos Jr., both houses of the Philippine Congress reiterated the urgency to ban the industry in the wake of a renewed spike in POGO-related crimes which reached 4,000 cases in the first half of 2023 alone. POGOs perpetrate crimes against other people or the public at large by means of online scams, frauds, unauthorized access to devices, and money laundering.

The digital age has transformed the way nations operate, communicate, and conduct business. While these advancements bring unprecedented opportunities, they also introduce significant vulnerabilities and threats. The Republic of the Philippines, like many other nations, faces an increasing number of cyber threats that jeopardize national security, economic stability, and the privacy of its citizens.

The National Cybersecurity Defense Act of 2024 is proposed to address these growing challenges by establishing a comprehensive framework for cybersecurity across the nation. This Bill aims to safeguard the nation's information and communications technology (ICT) infrastructure, protect critical information infrastructure (CII), and ensure a coordinated response to cyber threats.

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



CHARISSE ANNE C. HERNANDEZ

Republic of the Philippines
House of Representatives

19th CONGRESS
Third Regular Session

HOUSE BILL NO. 10797

Introduced by Hon. Charisse Anne Hernandez
Lone District of Calamba, Province of Laguna

AN ACT ESTABLISHING THE NATIONAL CYBERSECURITY DEFENSE PLAN 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 "National Cybersecurity Defense Act of 2024."

Section 2. Declaration of Policy. The State recognizes the vital role of information and communications technology in nation-building. It is the policy of the State to ensure the security and resilience of its cyberspace to protect against threats, mitigate risks, and safeguard the interests of the government, businesses, and citizens.

Section 3. Definition of Terms. For the purposes of this Act, the following terms shall be defined as follows:

a) **Cybersecurity** – Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

b) **Critical Information Infrastructure (CII)** – Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Section 4. Establishment of the National Cybersecurity Defense Plan (NCDP). The Department of National Defense (DND) in coordination with the Department of Information and Communications Technology (DICT), Philippine National Police (PNP), National Privacy Commission (NPC), and the National Bureau of Investigation (NBI) shall establish a National Cybersecurity Defense Plan (NCDP), in line with the National Cybersecurity Plan which shall

The NCDP shall be reviewed and updated every five (5) years to adapt to the evolving cybersecurity landscape.

Section 5. Components of the National Cybersecurity Defense Plan. The NCDP shall include, but not be limited to, the following components:

a) **Secure Government Network (GovNet) Infrastructure.**
   i. Development of a comprehensive cybersecurity defense system for all GovNet;
   ii. Integration of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Orchestration, Automation, and Response (SOAR), and Security Information and Event Management (SIEM) into GovNet.

b) **Establishment of Cybersecurity Defense Bureau.** I
   i. Strengthening of the National Computer Emergency Response Team (NCERT) and establishment of the National Security Operations Center (NSOC).
   ii. Expansion of NCERT to operate nationwide with capability for on premise incident response.
   iii. Modernization of the NSOC for centralized monitoring of government agencies.

c) **National Cybersecurity Threat Database.**
   i. Development of a national cybersecurity threat database accessible to the public.
   ii. Regular updates and categorization of threats based on the Common Vulnerability Scoring System (CVSS).

d) **Partnership with Public Telecommunications Entities (PTEs).**
   i. Collaboration with PTEs for early detection and mitigation of cybersecurity threats.
   ii. Establishment of minimum requirements for management of Customer Premises Equipment (CPE) and network segments for Internet Service Providers (ISPs) and telecommunications companies.

e) **Cybersecurity Workforce Development.**
   i. Establish a well-developed workforce to enhance the country's ability to engage with international partners, share information, and participate in joint efforts to combat cyber threats.
   ii. Ensure continuous learning and availability of skilled professionals
   iii. Be able to represent the country at international cybersecurity forums and contribute to global cybersecurity policies and standards.

f) **International Cooperation.**
   i. Expansion of bilateral and multilateral international cooperation in cybersecurity.
   ii. Participation in international cybersecurity forums and initiatives.

Section 6. Critical Information Infrastructure (CII) Protection. Be able to identify and classify CIIs using a risk based approach and establish CII Computer Emergency Response Teams (CERTs) for continuous monitoring and response.

Section 7. Prosecution of Cyber Offenders. The Department of Justice in coordination with the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall establish specialized units for the investigation and prosecution of cybercrime offenders.

The Department of Justice (DOJ) shall develop and implement guidelines for the swift prosecution of cybercrime offenses especially when the perpetrators are outside the Philippines, ensuring prosecution and imposition of appropriate penalties and sanctions in accordance with existing laws.

The government shall provide training for law enforcement officers, prosecutors, and judges on cybersecurity and cybercrime to ensure effective enforcement and adjudication of cybercrime cases.

Section 7. Funding. The amount necessary to implement the provisions of this Act shall be included in the General Appropriations Act (GAA) of the year following its enactment and thereafter.

Section 8. Implementing Rules and Regulations. Within ninety (90) days from the effectivity of this Act, the DND, in consultation with relevant government agencies and stakeholders, shall promulgate the necessary rules and regulations for the effective implementation of this Act.

Section 9. Separability Clause. If any provision or part of this Act is declared invalid or unconstitutional, the remaining parts or provisions not affected shall remain in full force and effect.

Section 10. Repealing Clause. All laws, decrees, executive orders, and rules and regulations, or parts thereof which are inconsistent with this Act are hereby repealed, amended, or modified accordingly.

Section 11. Effectivity. This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,